2020

A Novel Framework for Improving Cyber Security Management and Awareness for Home Users

Alotaibi, Fayez Ghazai S

UNIVERSITY OF PLYMOUTH

A Novel Framework for Improving Cyber Security Management and Awareness for Home Users

By

Fayez Ghazai S Alotaibi

A thesis submitted to the University of Plymouth
in partial fulfilment for the degree of

DOCTOR OF PHILOSOPHY

School of Engineering, Computing and Mathematics

August 2020

COPYRIGHT STATEMENT

Acknowledgements

First and foremost, all praise and gratitude are due to Allah the Almighty for giving me strength and helping me reach this stage of my PhD research and complete this important stage of my life.

I am deeply grateful for and my most sincere thanks go to my beloved mother, brothers and sisters for their great help, support, kindness and prayers for my studies. I am eternally grateful for your endless support and help. My sincere appreciation goes to the soul of my father and my brother (may Allah have mercy upon them).

I also owe many thanks to my wife, Sahar, and my children Yazeed, Ghanem and Yousef for their patience, endless support, and incredible care in assisting me throughout this endeavour. They all stood alongside me and provided me with an abundance of love and support, even when spending days, nights and holidays without me. I really appreciate your endless support and help on this PhD journey.

My special appreciation and sincere gratitude go to my supervisory team, Professor Nathan Clarke and Professor Steven Furnell for providing me with a wealth of help and encouragement during the PhD journey. Their experience, constant support, constructive feedback and professionalism in different aspects, such as their critical thinking, publications and presentations, have been helpful throughout my PhD journey and without their valuable comments and feedback, I would not have been able to reach this stage of my PhD, so thank you.

I would like to acknowledge, with thanks and appreciation, the government of the Kingdom of Saudi Arabia and my employer, Shaqra University, for granting me a scholarship and sponsoring my PhD study.

Last, but not least, I would like to thank the University of Plymouth and special thanks go to my colleagues and friends at the Centre for Security, Communications and Network Research.

Dedications

In memory of my father, **Ghazai**,

who left us in this world when I was 4 years old

and never lived to see his child

achieves his dreams and hopes.

In memory of my elder brother, **Ghanem**,

another father to us since the age of 13

who toiled for hope

but never lived to see it realised.

He passed away on 23rd July 2016.

Author's Declaration

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award without prior agreement of the Doctoral College Quality Sub-Committee.

Work submitted for this research degree at the University of Plymouth has not formed part of any other degree either at the University of Plymouth or at another establishment.

This study was financed with the aid of a scholarship from the Kingdom of Saudi Arabia - Royal Embassy of Saudi Arabia Cultural Bureau in London.

Publications:

1) Alotaibi, F.G., Clarke, N. and Furnell, S.M. (2020). A novel approach for improving information security management and awareness for home environments. *Information & Computer Security.*

2) Alotaibi, F., Clarke, N. L. and Furnell, S. (2019). Holistic Information Security Management for Home Environments. The 13th International Symposium on Human Aspects of Information Security & Assurance, HAISA 2019, Nicosia, Cyprus, July 15-16, 2019, pp.20–33.
   ISBN: 978-0244-19096-5

3) Alotaibi, F., Clarke, N. and Furnell, S. (2018). A Holistic Information Security Management Framework for Home Users. *International Journal of Intelligent Computing Research (IJICR)*, Vol.9, Issue 1, pp. 862 – 870.
   DOI: 10.20533/ijicr.2042.4655.2018.0105

4) Alotaibi, F., Clarke, N. and Furnell, S. (2017). An Analysis of Home User Security Awareness & Education. In 12th International Conference for Internet Technology and Secured Transactions (ICITST), Cambridge, United Kingdom (pp. 116-122). IEEE.
   DOI: 10.23919/ICITST.2017.8356359

Word count of main body of thesis: 57,055 words

Signed: ……

Date:……

Abstract

A Novel Framework for Improving Cyber Security Management and Awareness for Home Users

Fayez Alotaibi

A wide and increasing range of different technologies, devices, platforms, applications and services are being used every day by home users. In parallel, home users are also experiencing a range of different online threats and attacks. Indeed, home users are increasingly being targeted as they lack the knowledge and awareness about potential threats and how to protect themselves. The increase in technologies and platforms also increases the burden upon a user to understand how to apply security across the differing technologies, operating systems and applications. This results in managing the security across their technology portfolio increasingly more troublesome and time-consuming. Thus, it is apparent that a more innovative, convenient and usable security management solution is vital.

This thesis investigates current online awareness tools and reviews studies which try to enhance cybersecurity awareness and education among the home users. It is evident from the analysis that most of the studies which have made efforts in proposing "one-fits-all" solutions do not have the ability to provide the users with a tailored awareness content based on a number of criteria such as the current needs, prior knowledge, and security priorities for each user.

The thesis proposes an approach for improving security management and awareness for home users by providing them with a customised security awareness. A design science research methodology has been used for understanding the current problem, creating and developing an artefact which can enhance security management and awareness for home users. A number of security controls and requirements were identified which need to be managed and monitored for different technologies and services. In addition, the research designed several preliminary interfaces which can show the main components and aspects in the proposed solution based on HCI principles.

A participant-based study was undertaken to get feedback on the initial design requirements and interfaces. A survey of 434 digital device users was undertaken and reveal result that there is a positive correlation between the security concern, knowledge and management amongst home users towards different security aspects. Positive feedback and some valuable comments were received about the preliminary interface designs in terms of the usability and functionality aspects.

This builds into a final design phase which proposes a novel architecture for enhancing security management and awareness for home users. The proposed framework is capable of creating and assigning different security policies for different digital devices. These assigned policies are monitored, checked and managed in order to review the user's compliance with the assigned policies and provide bespoke security awareness. In addition. A mockup design was developed to simulate the proposed framework to show different interactions with different components and sections in order to visualise the main concepts and the functions which might be performed when it is deployed in a real environment. Ultimately, two separate focus group discussions, involving experts and end-users have been conducted in order to provide a comprehensive evaluation of the identified research problem, the feasibility and the effectiveness of the proposed approach. The overall feedback of the two discussions can be considered as positive, constructive and encouraging. The experts agreed that the identified research problem is very important and a real problem. In addition, the participants agreed that the proposed framework is feasible and effective in improving security management and awareness for home users. The outcomes have also shown a reasonable level of satisfaction from the participants towards different components and aspects of the proposed design.

Table of Contents

List of Figures

List of Tables

Chapter One

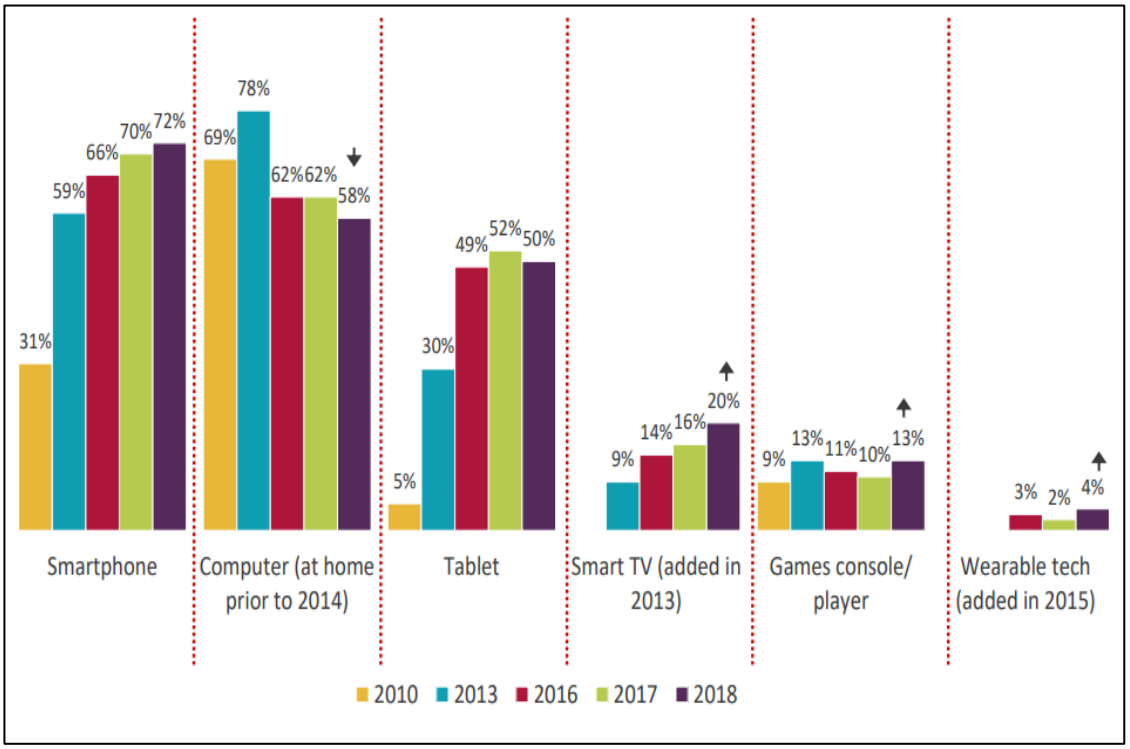
Introduction

1 Introduction

1.1 Introduction

The evolution of information technology is continuous and has become an essential part of our everyday life. Every home has at least one of these technologies from PCs, mobile phones, tablets and laptops to game consoles, smart TVs and the Internet of Things – each with different operating systems and a wide variety of online applications. ITU (2018) states that the number of internet users in the world rose from around 1 billion in 2005 to 3.90 billion in 2018. In addition, there are around 27 billion Internet of Things (IoT) connected devices worldwide in 2019, an increase from 7 billion devices in 2018 and it is expected to reach more than 75.44 billion devices by 2025 (Maayan, 2020). According to the Office for National Statistics (National Office of Statistics, 2018), 90% of households in Great Britain had internet access in 2018 including 81% of British adults using smartphones to go online, 63% use laptops and 57 % have tablets to browse the internet.

According to a study conducted by (Ofcom, 2019), the percentage of the UK adults who used smartphones rose sharply from 31% in 2010 to 72% in 2018 and tablet users dramatically increased from 5% in 2010 to 50% in 2018 as illustrated in Figure 1.1.



Source: (Ofcom, 2019)

Figure 1.1: Devices Used To Go Online By UK Adults from 2010 To 2018

According to the most recent Connected Consumer Survey from Google and TNS Infratest (Google, 2018), 30% of people in the UK own five or more digital devices. In addition, 33% the UK users have three to four connected devices. Worldwide, 7 billion connected devices were estimated in 2018, reached 26 billion IoT devices in 2019 and it is expected to reach more than 75 billion connected devices by 2025 (Maayan, 2020).

Alongside this significant increase in the number of Internet users using different platforms, different devices and a wide range of online applications and services, a significant increase in cyber-related threats has also been experienced (Taylo, 2015). A recent Internet Security Threat Report has published by Symantec (2019), overall web attacks on endpoints increased by 56% in 2018 and more than 1.3 million unique web attacks were blocked on endpoint machines every day. While the overall number of mobile malware infections fell during 2018, there was a fast increase in the number of

ransomware infections on mobile devices, up by a third when compared to 2017. Moreover, one in 36 devices were classified as high risk including rooted or jailbroken devices and malware had been installed on devices.

The above findings reveal that using new technologies and devices is increasing rapidly every year. In addition, the number of online threats and attacks is growing every day with home users increasingly likely to experience online incidents. A variety of reasons exist; including, they do not have appropriate knowledge and awareness which could help them to behave safely while going online, and whilst they are aware of online threats but they do not know the appropriate procedures required to mitigate the risk. Whilst solutions exist (as will be described in chapter 2 and 3) they arguably are failing to address the issue hence why users are still not understanding why, what and how to protect themselves.

1.2 Research Aims and Objectives

Focusing upon the burden placed upon users to understand and react to threats from a diverse set of platforms, operating systems and applications, the purpose of this research is to develop a framework for improving security management and awareness for home users. It will seek to unify the multi-device, multi-platform and pervasive threat environment into a usable single home-user security information manager.

In order to achieve this, the following objectives will be considered:

1. To critically analyse the current information security awareness tools and approaches and identify the research gaps and opportunities.
2. To develop a novel approach to mapping complex security requirements in an adaptable manner; being mindful of technologies, services and people.

3. To design and develop flexible usable interfaces that inform and engage users, enabling improved awareness and management.
4. To design a framework for improving information security management and awareness for home users.
5. To conduct a series of evaluations involving stakeholders in order to measure the practical effectiveness and the usability of the proposed approach.

1.3 Thesis Structure

Figure 1.2 presents and describes the stages which have been completed in this research in order to achieve the research objectives. This thesis is organised into nine chapters to fulfil the aims and objectives stated in the previous section, beginning by Chapter one that presents the research problem and summaries the overall research aim, objectives and the structure of this thesis.

Chapter two presents a review of the literature on information security awareness. Furthermore, it investigates the importance of information security awareness. It also provides an overview of the current methods used to raise information security awareness for home users.

Chapter three provides a literature review of the existing research and studies in information security awareness. Moreover, the chapter concludes with a discussion in order to identify the existing gap in the studies in order to highlight the lack of enhancing the information security awareness for home users by proposing information security policy approach for home users.

Chapter four is the research methodology chapter. It investigates some general research methods used in researches. In addition, it explains the research philosophy, approach and methodology used in this research to achieve the research objectives and aims.

Chapter five reviews the information security management frameworks and procedures which are proposed for organisations. In addition, it illustrates a number of best practice guidelines and recommendations which are offered for home users. A number of security policies including different security controls and requirements for different technologies are proposed in this chapter.

Chapter six presents a review of several HCI principles for designing user interfaces. In addition, it demonstrates several preliminary interfaces which can be used in the proposed system. Two alternative proposed interfaces are designed for each section in this study.

Chapter seven presents the results of a user survey conducted in order to address aspects of the problem that have not been covered by the literature in order to feedback on the final framework. It aims at exploring their security concerns, knowledge and management of different security controls and aspects. In addition, it includes the feedback of the participants for the proposed initial interfaces in terms of usability and functionality aspects.

Chapter eight presents a novel architecture for improving security management and awareness for home users. It describes its key components, functionalities and operational considerations. In addition. It discusses in detail a variety of different security policies which are applied in the proposed approach to provide bespoke security awareness content. A mock-up design is developed and explained, including a number of architectural aspects in order to ensure that the system is practicable in the real environment. In addition, it presents the evaluation feedback of experts and end-users about the proposed framework and the mock-up design.

Chapter nine is the final chapter highlighting the main conclusion of the research. It presents the achievements and limitations of the research. In addition, a discussion on the potential aspects of future work is provided in the chapter.

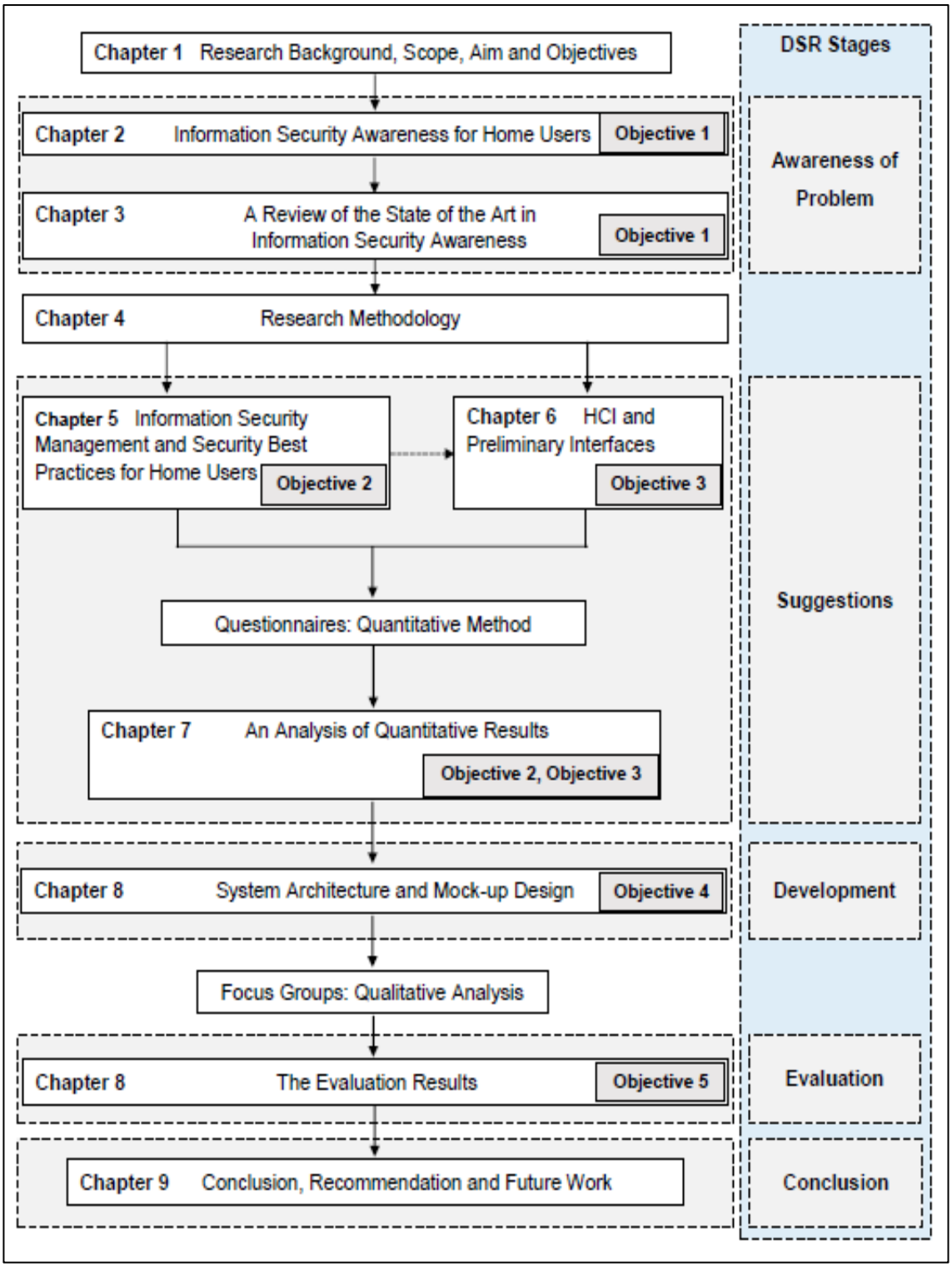


Figure 1.2: The Thesis Stages

Chapter Two

Information Security Awareness For Home Users

2 Information Security Awareness for Home Users

2.1 Introduction

With the rapid development of information technology including smartphones, computers, tablets, smartwatches and Internet of Things, providing security for home digital devices and services become more essential and more challenging as many home users face online threats and attacks (Nthala et al., 2018). Information security infinitives, procedures and literature have focused on technological aspects in order to provide a good security and protection level against cyber security threats without paying enough consideration to human aspects in information security (Ophoff and Robinson, 2014). However, technical aspects and solutions including security tools and systems cannot be used alone to provide the required level of security and protection of assets because these tools can become exposed and vulnerable to attacks and online threats due to user misuse (Furnell and Clarke, 2012).

In the organizational context, several standards, procedures and guidelines are used to implement a successful information security management by considering a variety of information security controls as well as human aspects in information security. The part of human aspects is dealing with knowledge, awareness attitude and behaviour toward different information security concepts, basics and threats (Kaur and Mustafa, 2013). However, it is necessary to make users aware of potential threats, risks and attacks and raise the value of information security awareness before implementing any security standards and guidelines because this can help users to understand the importance of these procedures and implementation which can make them more effective.

Home users do not have security policies, guidelines and IT staff which can help them in providing better information security in home networks. Therefore, home users are

responsible for providing the required protection for their personal digital devices and keep them secure all the time. The lack of managing security controls and settings properly and applying insecure practices can make home users exposed to a wide range of security threats and attacks such as malware attacks, identity theft, and phishing attacks (Alarifi et al., 2012; Furnell and Moore, 2014). Lack of security knowledge and awareness among home users is considered one of the obstacles which can prevent home users from protecting their devices and networks (Wash and Rader, 2011; Rao and Pati, 2012).

This chapter begins by providing some definitions of information security awareness, education and training in the next section. Section 3 discusses cybersecurity threats that can be experienced by home followed by reviewing the level of information security awareness around the world. The current information security awareness tools for home users are reviewed in section 5 followed by a discussion in section 6. Finally, a conclusion is presented in section 7.

2.2 Information Security Education, Training and Awareness

Information technology has become an essential part of the daily life activities of people which results in increasing the number of internet users, technologies, devices. This continuous increase makes the process of keeping end-users and their technologies secure more difficult and challenging. In addition, the dramatic increase of digital services and technologies leads to a significant increase in the number of online threats, breaches and issues. The importance of information security awareness has been strongly highlighted and underlined by many researchers (Haeussinger and Kranz, 2013; Bullée et al., 2015; Sherif et al., 2015). In the information security chain, users are often considered to be the weakest link (Howe et al., 2012). Therefore, raising and improving security awareness of home users is the first step in protecting and keeping them secure.

Wilson et al. (1998) define information security awareness as "Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly". Bowen et al. (2006) argue that the main objective of security awareness is to let users pay attention to information security aspects that can help end-users to recognise and identify the current threats and issues.

A conceptual analysis was conducted by Amankwa et al. (2014) based on the existing literature of information security. They found that information security awareness, education and training are different in terms of their focus, purpose and methods of delivery as illustrated in Table 2.1.

	Information Security Education	**Information Security Training**	**Information Security Awareness**
Focus	Insight and understanding.	Information security skills and information security knowledge.	Attention directing and reminders.
Purpose	Equip employees with the skills and competencies needed to ensure confidentiality, integrity and availability (CIA) of organisation information	Equip employees with information security skills and information security knowledge specific to their roles and responsibilities.	Every employee realise their role and responsibility towards protecting the organisation's information.
Method of delivery	Theoretical instructional methods in the form of seminars, classroom discussions and research	Practical instructional methods in the form of seminars and workshops.	Print and electronic media such as videos, flyers and posters.

Source: (Amankwa et al., 2014)

Table 2.1: Differences Between ISE, IST and ISA

Information security training is a key element in the information security domain. Providing users with the necessary security skills is the main goal of information security training. Training is defined by Wilson and Hash (2003) "Training seeks to teach skills that allow a person to perform a specific function". Bowen et al. (2006) argued that

understating the difference between training and society awareness is important in order to achieve the goals of each one. Therefore, the difference between training and awareness is that training focuses on teaching users skills, while awareness aims to allow users to pay attention to security issues (ENISA, 2010).

Education can be considered to be at the top of the learning development process. Bowen et al. (2006) state that "Education integrates all of the security skills and competencies of the various functional specialities into a common body of knowledge and strives to produce IT security specialists and professionals capable of vision and pro-active response". Therefore, it can be said that education aims to improve and enhance the ability of users to understand the importance and the necessity for different security activities, detect and take actions against information security threats and correctly implement security measures by improving their security behaviour.

All these learning procedures and processes are managed very well in organizations. However, it might be difficult to be implemented effectively for home users due to many reasons. First, home users have different security knowledge and skills. In addition, the lack of motivation in security awareness infinitives can make them less effective for home users. Furthermore, determining whether home users are well equipped and ready to go online securely or not is difficult, compared to organizational context because different security policies, tools, training and education courses and continuous security risk assessment and check are provided in the enterprise level (Furnell et al., 2008). This indicates that there is a need for prospering an approach which can enhance security awareness by telling users what they need to know about the threats, why they need to be protected from the threats and what they need to do stay protected (Furnell and Moore, 2014).

Herley (2009) stated that complex, long and growing sets of advice, instructions, policy updates and tip are offered to users. The author argued that people sometimes do not follow, ignore or reject the security advice because the value of the asset being compromised is less than the value of time that people have to spend on following the advice. Therefore, the actual harms and threats faced by users and their constraints need to be clearly understood in order to avoid rejecting or ignoring the security advice by. This can be achieved by providing them with bespoke information security awareness customised on users' current needs and requirements.

2.3 Cyber Security in Homes

The use of information technology in home has been taking an essential part. The number of technologies and IoT devices which are available for home users has been increased rapidly. The continuous increase in the number of IoT devices and developing smart cities has participated in providing home users a wide range of different digital devices and expanding the level of network which can be used in homes.

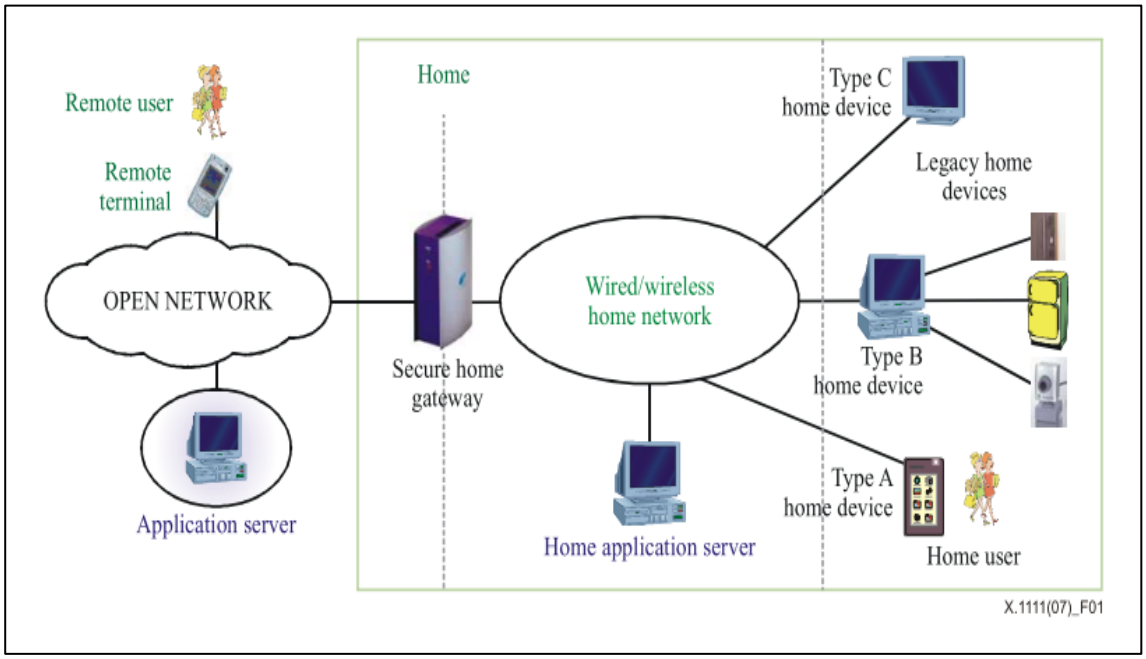
Different types of devices and technologies are used in homes such as computer (PC/laptop), smartphone, tablet, smart TV, game console, wearable devices, security system, monitoring cameras, and many more. These digital devices can connect to home network through wired, wireless or both connections.

According to Ofcom (2019), home users use their digital devices and technologies to access different online services including accessing email, internet browsing, instant messaging, VoIP services, banking, online shopping, social media, accessing news, watching videos, learning, government services, online games and file sharing. This continuous increase in using different digital devices with different platforms for

accessing a wide range of online services makes the management of information security and mitigating threats and issues difficult for home users.

ITU (2007) defines a general home network model for security which identifies all the entities and units in the home network and the relationship between the entities as shown in Figure 2.1. In the proposed model, the home devices are classified into three types based on its role:

- Type A home device: it includes devices such as remote controller, PC or PDA, which can control or manage the type B home devices or type C home devices.
- Type B home device: it works as a bridge that connects type C home devices which doesn't have any communication interface to the home network.
- Type C home device: it includes devices such as security cameras, A/V devices. It only provides some services to the rest of the home network devices.



Source: (ITU, 2007)

Figure 2.1: General Home Network Model for Security

2.3.1 Understanding Home Environment

Different concepts and definition have been provided for home which can be understood differently across different subjects and areas. Mallett (2004) stated that home is related to family, house, self and resort. Saunders and Williams (1988) described home as a real object (a socio-spatial system). They stated that the physical boundary such as a house cannot be used to define home. However, different relationships and activities can be enhanced and enabled in home by interacting with the physical elements in home.

Saunders and Williams (1988) stated that there is three different social spaces interfere with each other in home: household, family and neighbourhood. Hammel and Laslett, (1974) defined the households as co-resident domestic group which includes the people who live in one house. The authors reviewed the household and studied different classes of family as presented in Table 2.2. However, Saunders and Williams (1988) argued that the idea of linking the family to the household might not be perfect because people can be in the same household without being from the same family such as living in share houses, student accommodations and residential care home.

Categories	Classes
1. Solitaries	• Widowed • Single • Unknown marital status
2. No family	• Co-resident siblings • Co-resident relations of other kinds • Persons not evidently related
3. Simple family households	• Married couples alone • Married couples with child(ren) • Widowers with child(ren) • Widows with child(ren)

4. Extended family households	• Extended upwards • Extended downwards • Extended laterally • Combinations of the above three
5. Multiple family households	• Secondary units UP • Secondary units DOWN • Secondary units lateral • Frérèches • Other multiple family households
6. Incomplete classifiable households	

Source: (Hammel and Laslett, 1974)

Table 2.2: Composition of Households

ENISA (2010) defines home users as "citizens with varying age and technical knowledge who use ICTs for personal use anywhere outside their work environment. This user group can be further divided into different categories: kids, teenagers, youths, adult and silver surfers". Howe et al. (2012) states that home users can be considered to not be professionals in computing and digital devices.

2.4 Cyber Security Threats in Homes

Most home computers are vulnerable to cyber security attacks and threats because they believe that they do not have valuable information which can attract the hackers to attack them or they believe that they have enough cyber security and protection in their systems and devices. How*e* et al (2012) identified eight folk models of security threats used by home user to make decision about what security software can they use and what security advice they can follow. They found four distinct folk models about malicious software as a security threats such as viruses and other malware. In addition, they found four distinct folk models about hackers and break-ins. They stated that home users deliberately do not

follow security advice because they believe that it will not help them. They argued that security education efforts should effectively explain security threats which can be faced by home users in order to an effective understanding of threats. Security educations efforts should highlight why the suggested security advice and action are important and necessary rather than providing only a list of actions which need to be taken.

Therefore, home users should understand potential threats and attacks which might they face and how to mitigate these threats. Narayana Samy et al. (2010) classify three main types of threat sources which have different threats and incidents:

1. Natural: events and incidents which can be caused by forces of nature such as earthquakes, floods, earthquakes, tornadoes, landslides, and electrical storms.
2. Environmental: events or situations which can cause harm to the environment such as pollution, chemical spills, and liquid leakage.
3. Human: incidents and events which can be caused by human beings, including unintentional acts and deliberate acts.

Atamli and Martin (2014) argue that there are three main entities that can make a threat or danger to the security of IoT devices:

1) Malicious User: this is a user who owns an IoT device with the possibility to carry out an attack to discover the secrets of the manufacturer or access some restricted functionality or hidden features in the system. By doing this, the malicious user can get confidential information which can be sold to third party or to attack similar systems.

2) Bad Manufacturer: it is the manufacturer of the digital device that has the capability to utilize the device to collect and obtain information about the users, or other IoT devices used at home. Security holes can be intentionally designed in digital devices in order to access the user's data later. In addition, producing digital devices with poor security

specifications can lead to compromise the user's security and privacy. Moreover, by utilising the concept that the IoT devices can connect and communicate with each other, an attack can be launched by a digital device manufacturer on other competitors' devices in order to damage their reputation.

3) External Adversary: it is an external user or software which can gain access to the system without authorization. This type of user would try to obtain confidential information about the user of the system or device for malicious purpose such as causing financial loss, fault to the system or to be used in attacking other devices or systems via DDoS attack.

A wide variety of online threats and cyberattacks can be launched by organisations or individuals to attack and breach information systems and devices belong to another individual or organisation. Users usually get infected and exposed to online threats because they do not implement and manage their security control properly, they do not have enough security knowledge and security awareness about how to protect their network and digital devices from being exposed and attacked. There are several major security threats that can be experienced by home users and can affect home network security (Rao and Pati, 2012; Teymourlouei, 2015):

1. **Malware Attacks:** it is a malicious code which has the ability to copy itself to another program, files, boot sector or changing the computer performance. A device can get infected by a malware by clicking on a malicious executable file, browsing an infected website or removable storage devices. Malware has three common forms: spyware, viruses and worms.

2. **Password Attacks:** password security is important key to keep private information and systems protected. There are some methods of password attacks such as password guessing, password resetting, and password capturing.
3. **DDoS Attacks (Distributed Denial of Service Attacks):** this attack makes the device or the system is unavailable or inaccessible. The system must be able to be available and operate normally even if there is a malicious action. This type of attack can be launched by manipulating the device software or interrupting the connection.
4. **Pop-Ups:** cyber attacks can be occurred by making fake or malicious pop-ups. For example, a malicious pop-up can be shown to home users which can ask them to download and install untrusted software which can harm their devices and systems. Many popular internet browsers provide users with an option to activate pop-up blocker software to promote security and protection for home users.
5. **Operating System Vulnerabilities:** security holes and vulnerabilities which can be found in operating systems can be used to launch cyber attacks to gain access and steal private information from home user's computer. Software updates are regularly released to patch the current security issues in operating systems and applications. These updates can be done automatically and users can be informed when there is a new available update.
6. **Public Unsecured Wi-Fi Network Attacks:** using unsecured public Wi-Fi networks can make home users unsecured and steal their valuable information and passwords when the network is monitored by hackers.
7. **Phishing Attacks:** this type of attack is used to get sensitive data such as personal information, username, passwords and credit card numbers. This can be done by sending an email to home users who can be taken to illegitimate websites.

8. **Shoulder Surfing:** an attacker collects information such as password and PIN by looking at the victim's keyboard, screen or listening to a conversation.
9. **Lost or stolen end device:** it may happen more often to the devices carried such as smartphones and laptops. Loss, distraction or disclosure of stored information or data in the device can happen.

Nthala et al. (2018) state that all these threats usually are mitigated well in large organisations because they have security policies, segmented network architectures, firewalls, Antivirus, IDS, IPS, patching management, backup solutions and IT support team. In contrast, very few security resources, ability, knowledge, skills and tools are available to protect home users from a wide range of threats and attacks.

The lack of appropriate awareness, monitoring and management for the security configurations of the home devices could make them compromised easily and experienced security breaches which could be used to attack critical infrastructures and services such as telecommunication and banking and other organisations (Ng and Rahim, 2005). For example, X-Box Live, the PlayStation Network, Dyn (DNS provider), UK's TalkTalk and Post Office online services have been affected by a DDoS attack which was a botnet coordinated through a large number of Internet of Things (IoT) devices in homes that had been hacked and infected with malware(Lunsford and Boahn, 2015; Reynolds, 2016; Mahjabin et al, 2017). One of the ideal methods to mitigate the risk of these online threats and attacks is to educate users on how to keep their devices and information protected online and promote information security awareness level of users (Alarifi et al., 2012; Furnell and Rajendran, 2012).

2.5 Home Users Still Have A Lack of Security Awareness

Information security awareness and education have a key role in ensuring users are informed and educated on how to remain secure. Several studies have tried to assess the online safety and the information security behaviour of home users.

Several studies have tried to assess information security behaviour for home users. The National Cyber Security Alliance and McAfee (NCSA and McAfee, 2011) conducted a survey among home Internet users in the U.S in 2011, the findings show that 26% of the home users changed their passwords in the same week or month. However, 25% of the home users never changed their passwords without getting enforced by the service provider and only 15% changed them in the last year. In addition, 32% of the home users did not use any unsecured wireless networks while 53% used an unsecured wireless network to connect to the internet. A year later, another study revealed that 17% of the home users change their passwords for their social media accounts frequently (weekly or monthly) while 42% never changed their passwords for social media accounts. 31% installed security protection software on their smartphones compared to 64% who did not use any security software (NCSA and McAfee, 2012).

The online safety behaviour among American Internet users was also investigated and evaluated by NCSA and PayPal (2013). The results indicated that 32% the home users have a positive security behaviour for using different password across all their online accounts while only 8% used one password for all their online accounts. 34% used a PIN for their smartphones while more than half of the respondents (55%) did not configure PIN code to protect their devices. Around 48% of the home users said that all their apps are up-to-date while only 8% said one or two apps need to be updated.

Another study by Furman et al. (2012) to investigate and assess online security knowledge and skills for the US Internet users such as online activities, online fraud risk, computer security education and awareness, online security self-assessment, security mechanisms and home online security tools. The results revealed that the participants are aware of some coping mechanisms and security policies which might reduce the online risk and breaches but were not aware of how to deploy them effectively because they learned those protection mechanisms and advice from personal sources and life experiences. Moreover, the interviewees are willing and want to follow the right security practices in order to keep their devices secure.

Another study was conducted by Watson and Zheng (2017) to assess user awareness in the US towards mobile security. They found that around 20% of the participants did not configure any screen locking protection such as PIN or fingerprint. Around 80% used only the official app store to download apps while 20% used unofficial sources to download applications. 85% have never had a virus and around 62% have installed anti-virus applications. 44% of the users did not root their devices while only 12% rooted their devices and 44% were not sure about it.

A further study among UK adults highlighted that 55% were aware and used a firewall at home, 24% were aware but did not use firewall and 20% were not aware of the firewall. In addition, only 18 % of the mobile users used anti-virus software and a worrying 57 % were not aware of this security feature (Ofcom, 2015). Another study was conducted by Ofcom (2018) among UK adults highlighted that 41% used a firewall and 65% used anti-virus software in their devices. 55% used a strong password in their devices and only 34% did a regular backup. 40% downloaded the latest software updates when prompted.

The aforementioned studies analysed the situation of information security awareness in the USA and the UK which are considered as developed countries. The lack of cyber awareness is highly likely to increase among developing countries and nations because they do not have the appropriate infrastructure, enough budget and government support to establish information security awareness approach or campaigns which can promote security awareness. Rao and Pati (2012) conducted a study based on a survey which aims to evaluate information security awareness for home users in India. More than 80% of respondents used torrent.com to download software, games and movies. The results show 64% of home users did not use anti-virus software, 71% claimed that they were not sure about their security settings in their browsers, 80% indicated that they had no clue about malware, worms, spyware and phishing and 78% did not know about personal firewalls.

Chandarman and Van Niekerk (2017) assessed cybersecurity knowledge, skills, behaviours and attitudes by analysing 1231 responses in South Africa. 56% of the participants have a lack of knowledge about phishing and 43% do not know the purpose of antivirus software. Worryingly, 76% respond unsafely by opening a screensaver received by email. In addition, the result shows that the respondents have excessive trust in the content of their friends' emails. The feedback also indicates that targeted cyber security awareness is required as the generic common awareness campaigns do not improve cyber awareness effectively.

A survey of 629 participants was conducted by Alotaibi et al. (2017) to evaluate assess information security awareness in Saudi Arabia. The results reveal that most of 69% of the participants use their personal information such as date of birth and family names in creating passwords for different online accounts. A regular software update was done by only 54% and 35% back up their data regularly. The study found that the security

awareness of the threats and security practices is very limited although the participants claimed that they had good IT knowledge.

A further recent study evaluated security awareness and security practices among 802 Bangladesh users (Ahmed et al., 2018). The results show that 69% of the participants always use their personal information (e.g. last name, date of birth) for passwords and 59% of people always use USB devices in multiple devices. Worryingly, 77% have experienced and fallen victim of phishing emails, 71% have experienced online identity theft and 80% have infected by malware. However, the result shows a good level of cyber security awareness among the users as 91% acknowledge that people must not reveal their private information on the internet.

The above surveys and findings from different countries and regions including developed and developing countries have shown that a number of home users do not implement the best practices and do not manage their security controls properly. The reason behind this weak practice and poor management is that home users do not have enough knowledge and awareness which can help them in managing their security better (Furnell et al., 2008).

2.6 Current Information Security Awareness Tools for Home Users

Web-based portals are one of the most commonly used tools which are available for educating home users on how to use technologies in a good way in order to stay safe online. Another goal for the portals is to make people aware of the possible threats and the ideal procedures to mitigate these threats. The following most common cyber security awareness portals have been identified by searching in different search engines:

- **Stay Safe Online** (StaySafeOnline.org, 2019)**:** The website is developed and administered by the National Cyber Security Alliance (NCSA). It attempts to promote

online security awareness among the public by providing security tips to protect devices, personal information and children online activities. In addition, the website offers some free security quizzes, games and tools. NCSA also organizes campaigns such as STOP.THINK.CONNECT and the National Cyber Security Month. The website provides security awareness content for only a few devices without being classified based on the user age or knowledge. Furthermore, there is no attempt to evaluate the security knowledge of the users or to manage their improvement.

- **Microsoft YouthSpark** (Microsoft, 2019)**:** Microsoft has started a YouthSpark initiative to provide free computer education courses. One of these courses is to provide resources in order to enhance online safety among families. The website contains tips and advice delivered through such as videos, posters, presentations, guidelines and quizzes. However, YouthSpark is not a separate portal but it is linked with Microsoft's website which makes it difficult for parents and teens to find it. In addition, the website does not have an internal search tool and menu which makes it difficult for the users to find particular information. Another drawback is that the information is not sorted properly (children, teens and parents in one page).
- **Get Safe Online** (GetSafeOnline.org, 2019)**:** Get safe online is one of the well-known sources for online safety. This website provides practical advice and tips to public people about how to protect themselves, computers, smartphones, tablets, safeguarding children and guidance to use social networking, shopping banking and payment websites safely. In addition, the website offers virtual assistant called "Ask Terry" which helps the users to get answers for their questions about information security as shown in Figure 2.2.

Source: (GetSafeOnline.org, 2019)

Figure 2.2: Ask Terry Service in Get Safe Online Website

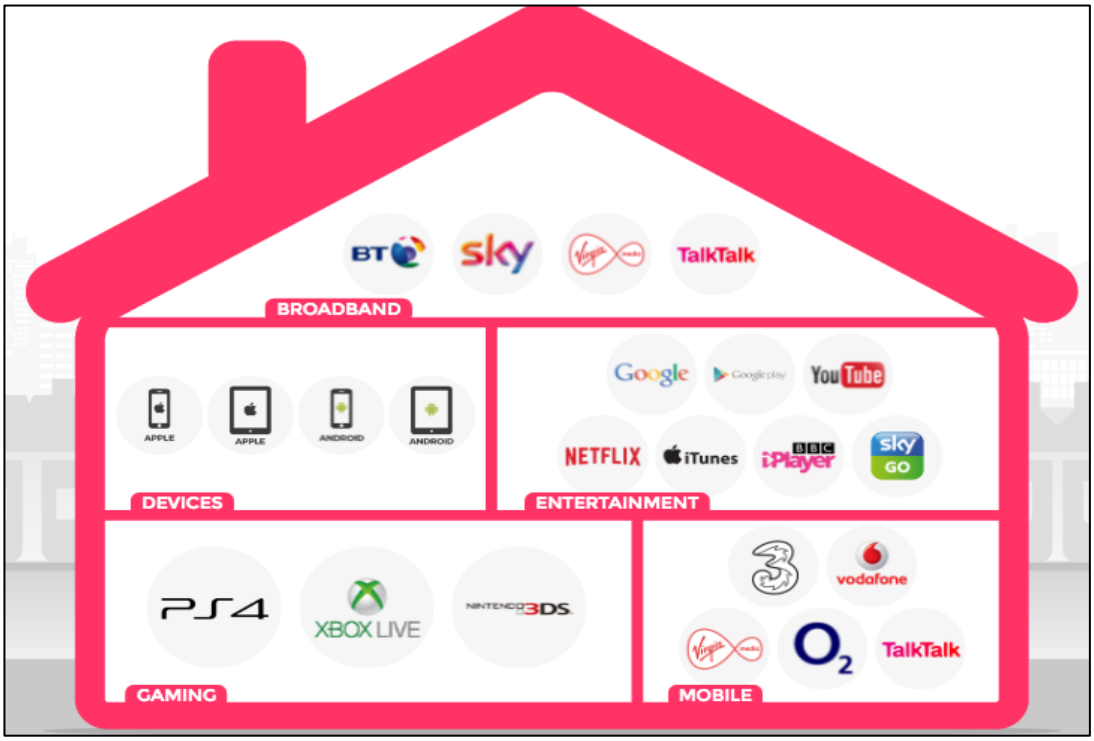
- **Google Safety Centre** (Google, 2019)**:** The website provides awareness information for family members about online safety including tips, advice, resources and safety tools. However, the website is very basic and does not provide any type of monitoring or reporting. In addition, the information is not categorized based on the age of the user and it does not provide awareness topics suitable for children. Furthermore, the safety centre portal is linked with Google's main website which could make home users struggle to find the portal.
- **Norton's Family Resources** (Norton, 2019)**:** This website includes videos, articles and a blog which assisting in keeping family members protected online. Moreover, it has a family online safety guide which covers all the ages from 3 to 17 years. As a leading provider's security software, the offering which has been made to support and inform end-users is limited, poor and difficult to locate because the portal is connected with Norton's main website. Furthermore, it does not provide comprehensive

resources for families due to the lack of material and information related to online safety.

- **The UK Safer Internet Center** (Saferinternet.org.uk, 2019)**:** the resources and information on the website are classified into four groups: young people, parents, teachers and social workers. In the group of young people, the resources are categorized into: Resources for 3 – 11 and 11 – 19 years old, which contains games, videos, quizzes and advice to behave safely when using the internet. However, the website does not manage or monitor the users such as providing a report about their knowledge and progression. In addition, the website did not attempt to provide the contents based on the level of user knowledge.
- **Connect safely** (ConnectSafely.org, 2019)**:** the website is provided by Connectsafely which is a non-profit organization which aims to spread the principles of online security awareness among the public users. It offers security tips, advice and guides for the home users. It also provides guides for parents and educators about the best practice of online security. However, tips and advice are not sorted based on age groups such as kids, teens and parents. Furthermore, the website does not provide any types of attractive methods in order to be used interestingly among kids.
- **Wired Safety** (Wiredsafety, 2019)**:** the website provides a wide range of advice and tips for online safety. For example, people can read advice about how to protect the family members from cyberbullying, email spoofing and online shopping. Moreover, the website offers help and support services for people who need help and advice for online issues. On the other hand, the website only uses written tips and articles to deliver the knowledge and information, it does not use games, videos, quizzes or any other methods to attract all the family members. Moreover, the website contents are not organized based on the age of the knowledge level. The usability of the website

is poor because of some findings such as there is no internal search tool and the website topics have not been updated since March 2016.

- **The Irish Internet Safety Awareness Centre** (Webwise, 2019): the Iris Internet Safety Awareness Centre develops many resources which can promote Internet safety among young people. The website provides information and advice for parents and teachers. For example, parents can download guides in cyberbullying, social networks, new media technologies and internet filtering. However, most of the materials are focusing on parents, only one book called Play and Learn which is suitable for kids to learn the e-safety concepts.
- **Safe and Secure Online** (SafeandSecureOnline.org, 2019)**:** the educational program is funded by (ISC)2 and it aims to provide programs which can raise the cyber security awareness among communities. People can download materials about online banking, computer protection, data backup and safe passwords. However, it does not cover a wide variety of technologies such as PCs, laptops and security settings in different platforms.
- **Internet Matters** (Internetmatters.org, 2019)**:** it is a non-profit organization which aims to provide a safe environment for the children in the digital world. The website discusses many issues related to the Internet and devices. In addition, home users also can find advice classified based on age groups. Moreover, privacy and prenatal control guide for mobile devices, entertainment devices, video games and broadband modems, which are presented in an interactive design as shown in Figure 2.3.



Source: (internetmatters, 2016)

Figure 2.3: A Parental Control Guidance for Home Devices

Once the user can click on the required device, a step-by-step guide will be shown for the users in order to apply some restrictions. However, the guidance only helps the users to block the access to applications, camera and inappropriate content on the web without any support to enable the security features such as encryption, strong password and patches.

- **Childnet International** (Childnet, 2019)**:** it is dedicated to assist young people to use Internet technologies safely. The website topics are divided into some groups: young people, teachers and parents. Many online issues have been addressed in the website such as online gaming, cyberbullying, security and privacy awareness. The website is very usable in terms of the navigation, architecture and content.

According to the above analysis review of the current cyber security awareness websites which are available for public and home users. A number of security awareness portals

are analysed and reviewed based on the following criteria: methods used to deliver awareness for the users. The platforms which are covered in the portals and whether they provide different awareness for different age groups or not. Table 2.3 presents an analysis of the cyber security awareness portals based on these identified criteria.

		Get Safe Online	Stay Safe online	Microsoft YouthSpark	Google Safety Centre	Norton	UK Safer Internet	Connect safely	Internet Matters	Wired safety	Webwise	Safe & Secure Online	Childnet
Platform	**Generic Information**	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	PC	✓		✓									
	Laptop	✓							✓				
	Tablet	✓					✓		✓		✓		
	Smartphones	✓	✓	✓			✓	✓	✓				
	Game Console			✓			✓	✓	✓				✓
	Smart TV	✓					✓		✓		✓		
Age groups		✓					✓		✓			✓	
Content	**Quiz**	✓	✓				✓		✓				✓
	Games		✓				✓						✓
	Infographics		✓									✓	
	Videos	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
	Presentations			✓			✓	✓			✓	✓	✓
	Checklists			✓			✓		✓		✓	✓	✓
	Leaflets	✓							✓				
	Posters		✓	✓									

Table 2.3: A review for the cyber security portals for home users

In addition, there is an effort has been made to enhance cyber security and online safety among children. The European Commission launched a strategy for a Better Internet for Kids (BIK) in 2012 which aims at providing better integrated and more effective support for children when they go online and increase access to high-quality content for children

and young people. The BIK core service platform allows exchanging knowledge, expertise, resources and best practices between the European safer internet centres (SICs) and to provide services to their user (BIK, 2020). Anther project called EU Kids Online project, which is funded by BIK, which is a multinational research network that tries to improve knowledge of European children's online opportunities, risks and protection (EU Kids Online, 2020).

Several initiatives have been launched to prompt online safety teaching in schools in order to make sure pupils understand how to stay safe and behave online. The Department for Education (2019) has released and published guidance which must be used across the UK schools. The guidance highlights the importance of safeguarding children and young people from risky and inappropriate online materials. It supports schools to teach their pupils how to stay safe online within new and existing school subjects. In addition, Safer Internet Day is a global campaign which is celebrated every year in many schools and colleges to promote the safe and responsible use of technology and try to enhance online safety amongst young people, parents, carers, teachers.

2.7 Discussion

A wide range of online threats can be experienced by home users and affect the protection of their devices and networks. Several studies, which assessed information security awareness for home users in different regions and counties, indicate that home users do not have enough security knowledge, and they do not manage their security properly. This implies that users are not educated and prepared properly to make the appropriate security decisions when they are needed (Kritzinger and Von Solms, 2010; Furnell and Clarke, 2012; Furnell and Moore, 2014).

A wide variety of information security awareness portals are available for home users. These portals may be considered as a good resource for users who know what they need and look for particular answers. However, they generally have the following drawbacks:

- Most of these resources provide generic information and basic knowledge for beginners and novices which might not be useful for some users who have different skills or issues.
- Most of the websites provide long written tips and advice with some limited videos and games which might frustrate the users to interact and read the awareness contents.
- Some portals offer some advice and tips for a few technologies. For example, the websites of Norton, Google Safety Centre and Wired Safety offer general tips without attempting to provide awareness advice for particular technologies such as smartphones, tablets and game consoles.
- They are generally not well organized and structured. For example, the above three websites are not separate websites but they are linked under the main website of their companies which could make it difficult for people to find them.
- There is a noticeable lack of the motivation in most of the portals. A few quizzes and games have been offered but they did provide bespoke security knowledge and awareness based which can meet the user's current level which can make it more effective and useful.

There are however some good points in some portals. For example, the way that the Internet Matters website shows the parental control guidance for home users is very attractive which can encourage the family members to interact with the website by allowing them to select all the devices connected to the home network in order to get the

required security guideline as shown in Figure 2.3. This is will provide the users with tailored guidance based upon the selected device which can save their time and efforts.

2.8 Summary

This chapter has focused on information security awareness for home uses and current related issues. Several events and studies from different counties which have been reviewed showed that home users suffer from different issues in information security awareness such as lack of security knowledge, lack of understanding the security concepts, the lack of willingness to manage and monitor different security settings across different devices which makes them more vulnerable to many threats and attacks. The current information security awareness tools and initiatives such as web portals are one size fits all solutions which might be less effective and need to be improved by taking into account user's knowledge, skills, current needs and reflecting meaningful information in an adaptive and usable manner in order to raise people's cyber security awareness. The next chapter explores and reviews the academic literature within the information security awareness domain – specifically focusing upon work relevant to home users.

Chapter Three

A Review of the State of the Art in Information Security Awareness

3 A Review of the State of the Art in Information Security Awareness

3.1 Introduction

This chapter seeks to explore the academic literature within the information security awareness domain – specifically focusing upon work relevant to home users. The chapter begins with discussing the criteria which will be used to analyse the academic studies. The chapter will be concluded with a discussion section which will provide an understanding of the gaps that remain in the area of information security awareness for home users.

The studies and approaches which are identified in the literature review will be analysed and reviewed based on different aspects such as:

- The main concepts and methods used in the approaches to deliver information security awareness and management.
- Whether the solutions are able to provide customized and bespoke security awareness based on the current need of users.
- The awareness content in the tools is evaluated based on the awareness contents, subjects and the online threats which are discussed and delivered to the users.
- Whether the usability and functionality aspects have been evaluated by the stakeholders or not.
- Whether they provide any features to encourage and motivate users to use the tool in order to enhance their cyber security awareness or not.

3.2 Literature Review of Information Security Awareness Approaches

A number of studies and approaches have been identified within the information security

awareness domain. These approaches have been reviewed and categorised into four domains based on the scope of security awareness which they delivered:

- General security awareness: it includes the tools which provide general security awareness about different issues
- Security guidelines and controls: it contains the solutions which can control security settings and provide a security guideline for users.
- Web threat awareness: it has the tools which provide security awareness for web threats and using browsers securely.
- Gamification: this group includes solutions which provide security awareness by playing games.

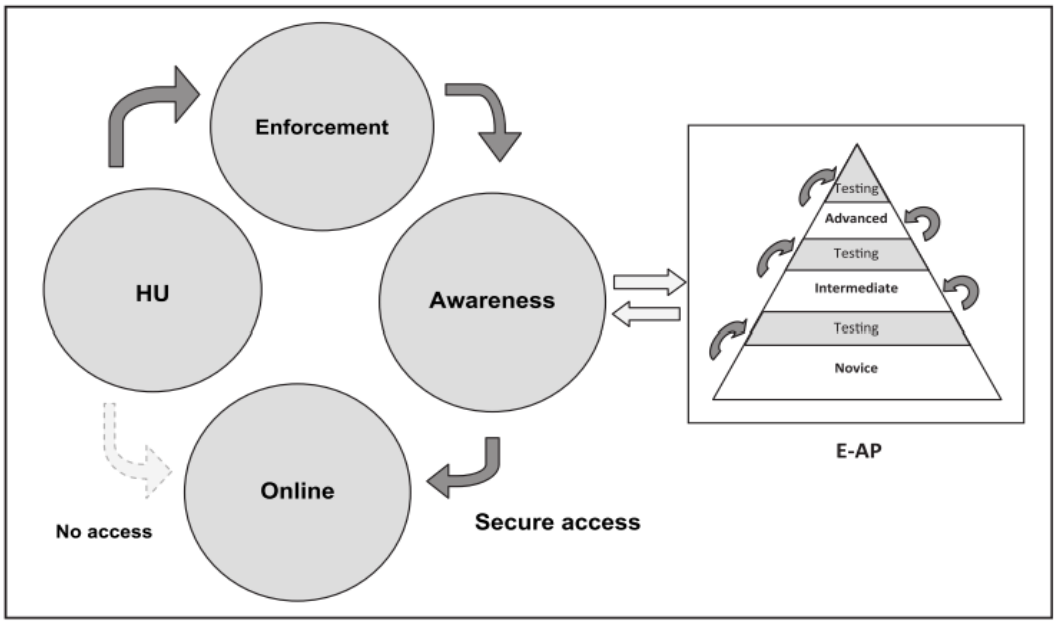
3.2.1 General Security Awareness

Some issues related to the quality of the current information security awareness programs and courses for home users were discussed by Kritzinger and Von Solms (2010):

- Resources do not cover all the most important cyber security issues.
- It is not easy for novice users to find those resources.
- The available programs only provide basic security information and knowledge without testing the current user's knowledge to provide a suitable level of knowledge.
- Some of the awareness resources are not updated regularly.
- Home users are not enforced technically to join the awareness programs.

Therefore, they proposed a theoretical E-Awareness Model (E-AM), which contains two components: the awareness and the enforcement component. The awareness component (E-Awareness portal) contains useful materials and awareness courses. These topics are classified based on the level of the home user knowledge which is divided into three

levels: novice, intermediate and advanced and the users can be evaluated and tested in each level. In the enforcement stage: they suggest that the portal can be hosted in with regulating services such as information services providers (ISP) to ensure that all the users cannot access the Internet without accessing E-Awareness portal as it is illustrated in Figure 3.1. The authors claim that they are working on a prototype and it will be tested later. However, they have not provided anything yet that they might face some financial, technical or organisational issues prevented them from developing a prototype.



Source: (Kritzinger and Von Solms, 2010)

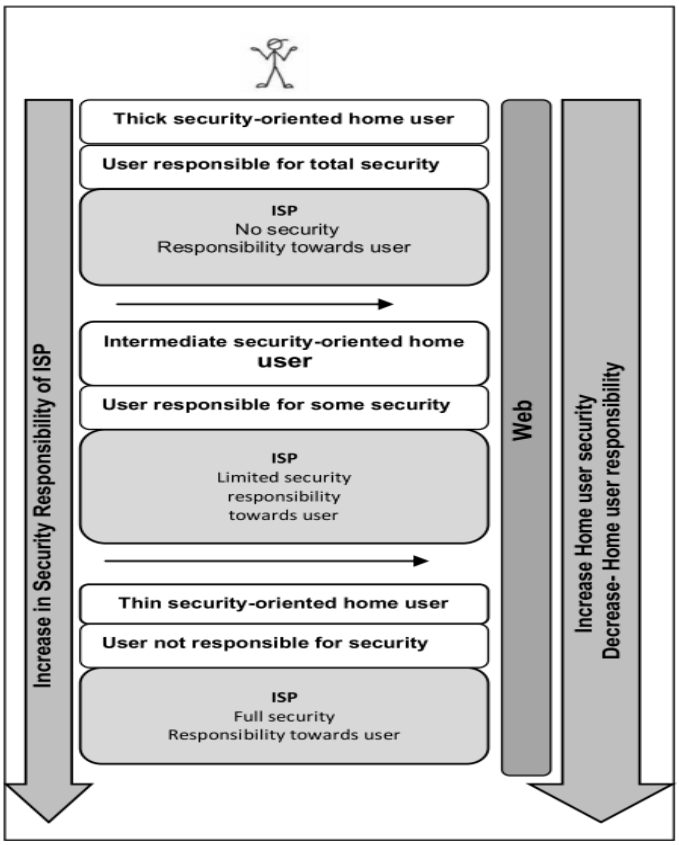
Figure 3.1: The full E-Awareness Model (E-AM)

Two years later, Kritzinger and Von Solms (2013) suggested theoretically a technical approach that can move the technical security protection responsibility (firewall, strong password, anti-virus, updates, patches) from home users to ISPs by following three approaches: thick, intermediate and thin security-oriented home users:

- Thick user level: the cyber security responsibility is totally handled by home users.
- Intermediate users level: the responsibility is shared between home users and ISP
- Thin users level: ISPs are responsible for all the cyber security tasks related to

home users.

They argued that providing security for home users is becoming more effective if the responsibility is migrated from home users to ISPs because all the security tasks will be handled by technical experts in ISPs which could decrease the risk level as it is illustrated in the approach framework in Figure 3.2. This approach only works as a protection tool without providing home users with security awareness or topics which could promote users knowledge about cyber security threats.



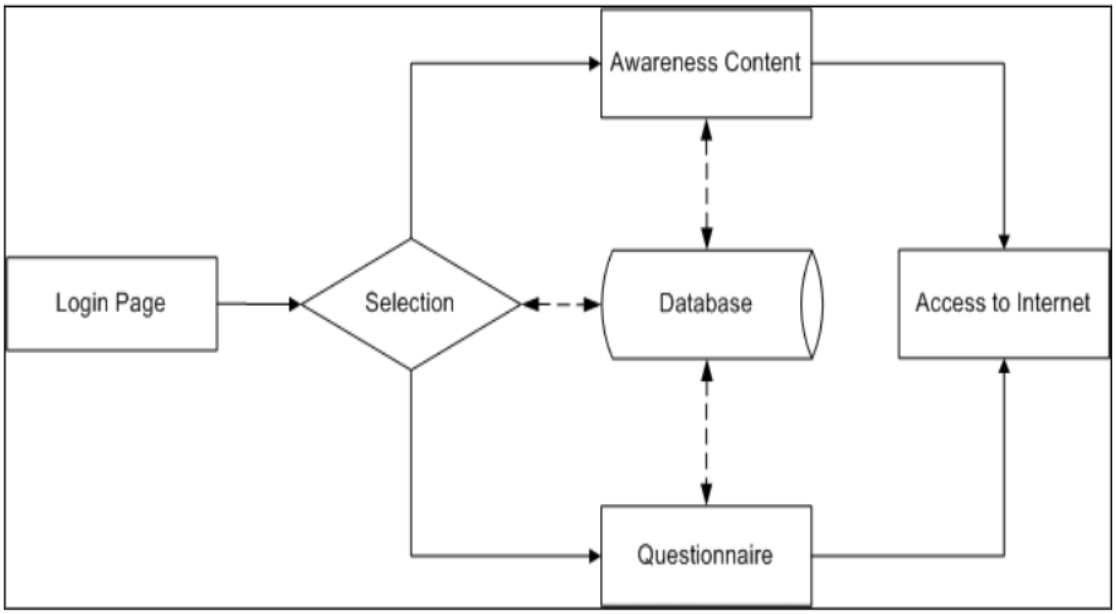
Source: (Kritzinger and Von Solms, 2013)

Figure 3.2: The Home User Security Framework

Supposing that ISPs will take the responsibility of providing security management and awareness for home users, this can make an extra effort and tasks by monitoring, managing and configuring with different technical controls and settings with multiple devices connecting via different ISPs. Moreover, an additional financial cost has to be paid by home users for providing this service. In addition, this type of restricted

enforcement might annoy and disturb the users' online activity. Additionally, this type of intervention from ISPs might make some privacy issues because ISPs will store and deal with confidential information for home users and their devices which can be breached and exposed which put home users at risk and start blaming ISPs for any issues which might happen for their devices and information. These issues might lead them to reject this approach or try to bypass the portal.

Labuschagne & Eloff (2012) claimed that many internet users use shared resources and computers in some African rural areas and they are not aware of online risks and threats. Therefore, they decided to use the point of shared devices as a positive point and proposed a Shared Public Security Awareness (SPSA) system based on a virtualized environment. SPSA system architecture consists of some components and each component has a particular task as shown in Figure 3.3.



Source: (Labuschagne & Eloff ,2012)

Figure 3.3: Internet Access Systems in SPSA

The system tried to prevent the users from using the internet if their level of security knowledge is not satisfactory but the proposed awareness contents are not provided based

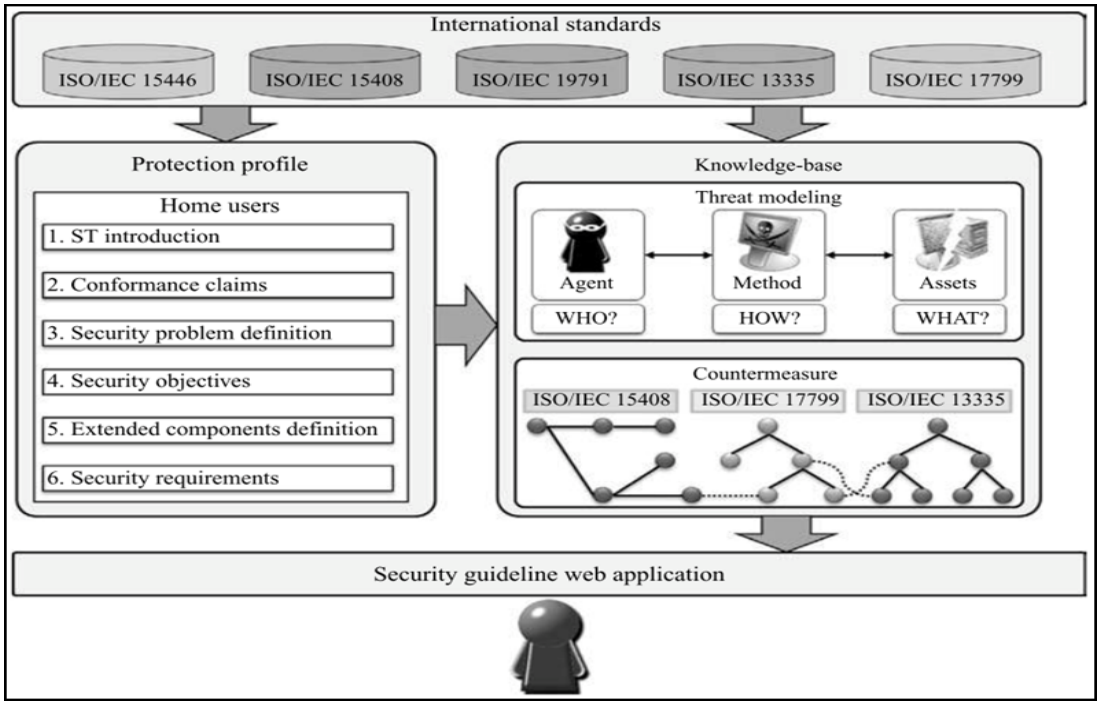
on their needs which might be generic and not useful for them. In addition, this approach does not have centralized management as it is proposed to work only with shared computers on virtual platforms. Therefore, the tool is required to be installed on each computer by the administrator account manually in order not to be uninstalled by the users. In addition, the process of collecting the behaviour report and updating the awareness content is done manually in each platform and each device. Another negative point is that the system is very limited as it only works with the browser tasks on shared computers so when using other internet services or applications on different popular devices such as smartphones, game consoles and internet of things, the user is not enforced to the awareness system.

Tolnai & Von Solms (2009) proposed an Information Security Awareness Portal (ISAP) used as an educational source to learn about online threats. The proposed portal consists of several limited categories such as the internet, online transactions, countermeasures and a forum. Another portal was designed by Smith et al. (2013) which aims at providing awareness of social engineering threats and risk including materials and quizzes. The quizzes are divided into different levels in order to motivate and encourage the users to answer them. These two approaches have the same issues of the awareness portals and websites by providing general cyber awareness without being customised based on the current needs of the users.

3.2.2 Security guidelines and controls

Another approach was proposed by Caceres & Teshigawara (2010) to design a security guideline tool for home users based on international standards to help them to understand the online threats and allow them to select a suitable security policy. This approach has three main components as shown in Figure 3.4:

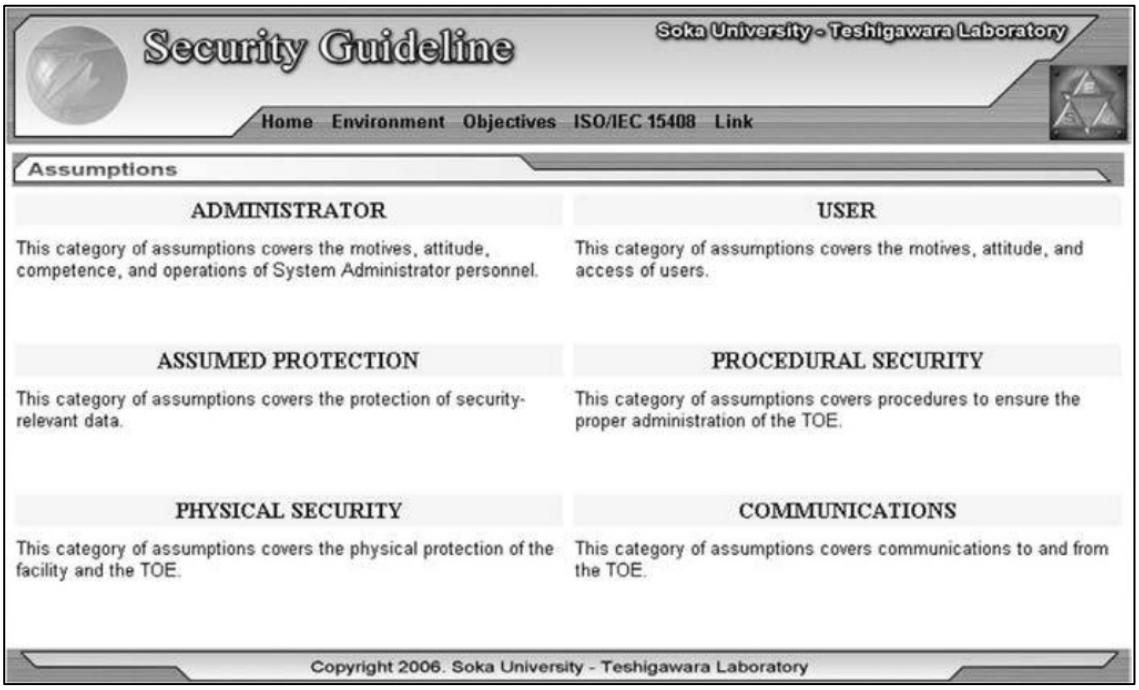
- Protection Profile (PP): it is based on international standards and allows the users to understand the security issues and to be used as a guideline for home users.
- Knowledge-base: it is created based on the PP. In addition, it contains 76 threats and 150 countermeasures which can be used in the home user environment but it seems that the database needs to be updated and maintained manually.
- Security Guidelines Web Application interface: it is the front-end user interface which allows the user to browse the required information about threats in the tool.



Source: (Caceres & Teshigawara, 2010)

Figure 3.4: Architecture of The Security Guideline Tool

Several steps must be taken by users to get the required security policy. The first step is that the users access the Security Guideline Web portal which categorizes the threats into different sections as shown in Figure 3.5. Next, the user should select one of the security objectives in each threat: prevention, detection or correction. Finally, once the threat and security objective is identified, the user will be able to have a security guideline which could mitigate the risk.



Source: (Caceres & Teshigawara 2010)

Figure 3.5: The Security Guideline Web Interface

The proposed tool was installed on a server in order to be evaluated by the users. A number of users mentioned that their cyber security knowledge about online threats improved from 52 % to 90%. In addition, 85% of the users believe that the proposed system will be beneficial for users in order to mitigate possible online threats. The tool only covers five categories of online threats.

The authors mentioned that the system will help the users to prevent, detect or correct the issues but they do not explain how the guidelines and policies will be collected from the knowledge base and international security standards and how it will be presented to the users for each objective. The approach requires some information which needs to be provided by the users such as the symptoms of the threats, which means it might not be useful if the user is not aware of the current threat. In addition, it seems that the proposed system does not have the ability to manage and monitor the users which could help the administrator to evaluate security behaviour for each user and the experienced online threats. Furthermore, the approach is designed based on particular security standards

which mean the threat which is not mentioned in the standards will not be included in the guideline. Moreover, the first page of the tool indicates that there is no attempt to attract and motivate users to use the tool.

Risk assessment is an essential process for making users aware of online threats because it provides a continuous activity of identifying hazards and risk that might cause harm to digital devices and users. Magaya & Clarke (2012) claimed that the current risk analysis tools are designed for organizations which might not be appropriate for home users due to the cost and technical experience requirement. Due to the basic generic information provided by cyber security awareness portals, they proposed a web-based risk analysis tool (WEBRA) for home users which is easy to use and does not require practical skills. WEBRA tool is designed to use ISO 27002 and NIST SP 800 – 30 standards in order to specify the implemented assets and controls. The tool consists of four parts, the first task is that the users are asked to select the device they have, controls and services implemented on their devices in order to create an asset profile. The second step is to analyse the user behaviour and awareness by answering 18 questions in different topics such as passwords, backup and encryption. Another process is that the risk of the missing controls is analyzed and prioritized based on the CIS 20 Critical Security Controls (CIS, 2016). Next, users are provided with a recommendation page which contains recommendations and links to websites in order to help them to implement the required security controls.

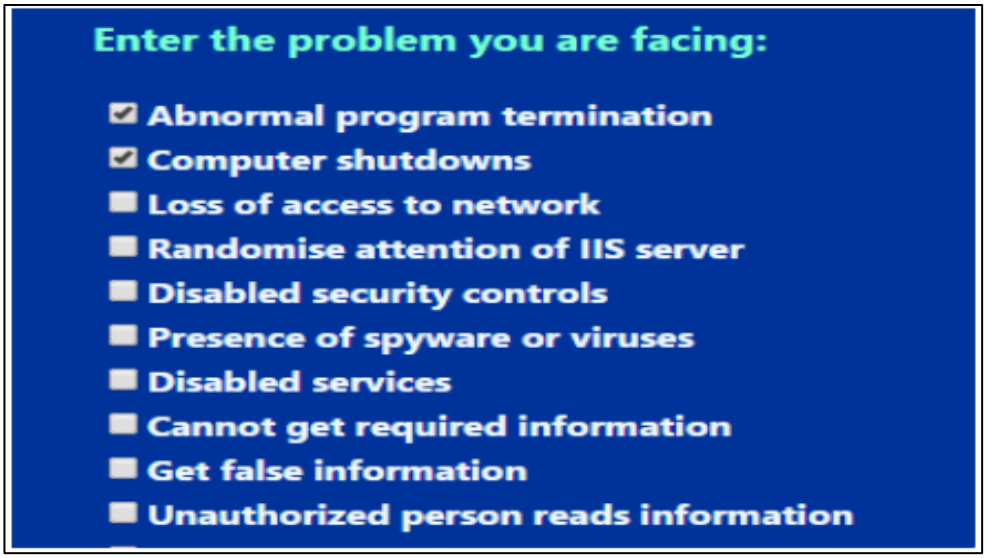
In general, The users' feedback about the tool is good in all the aspects, 93% of the home users said that the tool was easy to use, 81% found the system was very helpful, 78% stated that the tool was very good to improve their security awareness. The tool tried effectively to provide the home users with tailored recommendations based on online

behaviour and the missing controls in order to save time and effort and provide efficient guidance. However, the process of detecting the controls and service currently implemented is done in a manual way from the user side which could be difficult for some novice users. Moreover, the tool does not have the ability to check the effectiveness of each implemented control. For instance, if the user selects that the password is configured, the tool will exclude it from the missing control list without identifying the password strength which might be weak. In addition, it does not have any kind of motivation which could encourage the home users to follow the best practice. For example, when the tool finds that the result of the risk assessment for the user is satisfied, the user can be rewarded with a score or digital badge.

An alternative approach to inform the home users on online attacks awareness and the prevention procedures which is called Quick Reference was introduced by Teymourlouei (2015). The reference guide tries to identify the most popular online attacks such as malware, password attack, DDos attack and phishing scams. In addition, it provides 18 security steps which can be applied to enhance home user's cyber security. However, this approach provides only a fixed written reference with a list of countermeasures, similar to what the awareness portals provide which might not be usable and convenient for home users.

Rani & Goel (2015) designed an Expert System for Cyber Security Attack Awareness (CSAAES) to raise cyber security attack awareness among internet users and assist them to identify and solve the issues that their computers experience such as viruses, social engineering, SQL injection and data modification. In the first page of the system, there are two options to be selected by the users: attack identifier and information about a specific attack type that the user would like to get more information about it. The attack

identifier provides a checkbox list which contains 25 symptoms which might the user face some of them as shown in Figure 3.6.

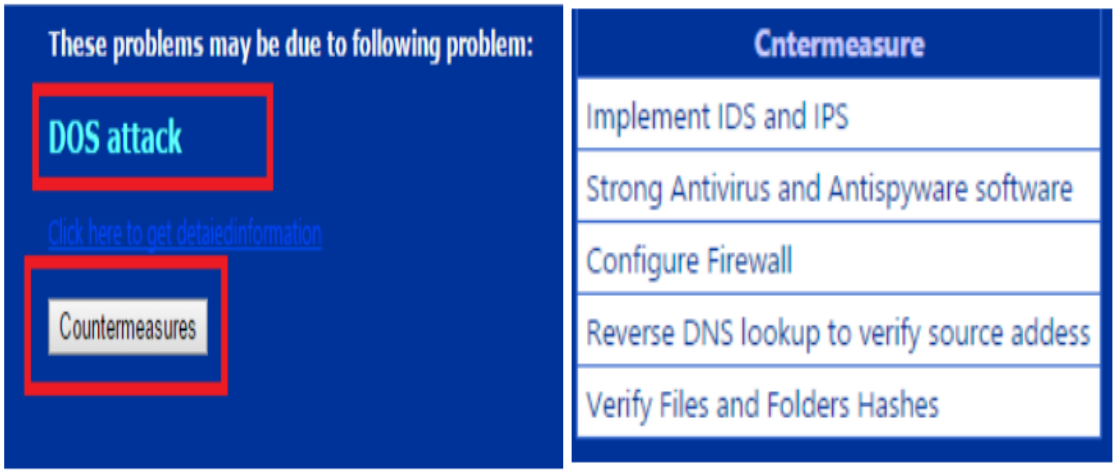


Source: (Rani & Goel, 2015)

Figure 3.6: Selecting Symptoms Faced

Next, users are provided based on the selected symptoms with the following: the possible attack type (18 types can be identified), more information about it and countermeasures to deal with the attack properly as shown in Figure 3.7. The system is tested with different scenarios and it is performing correctly but it is not evaluated in terms of the usability and functionality aspects. However, the tool requires some symptoms which might be difficult for home users to provide them due to their poor knowledge. In addition, the tool might not be accurate in identifying the threat because many threats have the same symptoms. The suggested countermeasures are provided without a guideline on how to implement each countermeasure. For instance, the system suggests that users should configure the firewall in Figure 3.7 but it does not provide any guidelines to show the user how to configure the firewall. Most of the provided symptoms are not compatible with tablets, smartphones and the Internet of things. Moreover, the system has some concerns related to the design and usability. For example, the background colour used in Figure 3.7 is dark blue and the sentence: “Click here to get detailed information” is written in blue colour

as well which makes it difficult to be seen.



Source: (Rani & Goel, 2015)

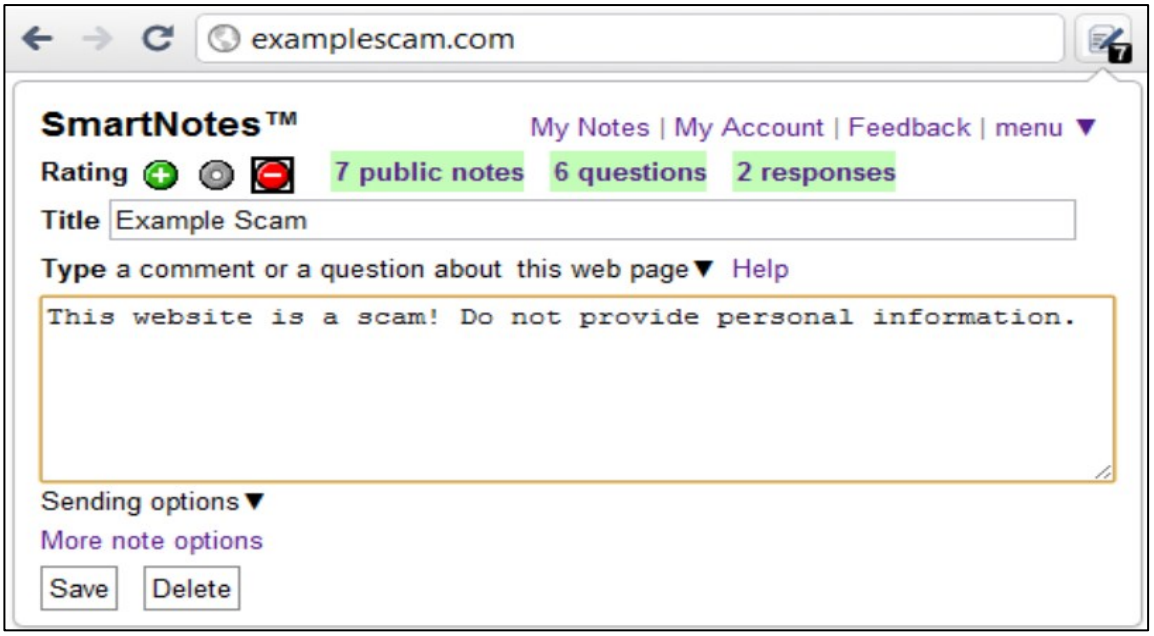
Figure 3.7: Attack Present and Countermeasures

3.2.3 Web threat awareness

Browsing the Internet and online services can facilitate many tasks in our daily life activities. However, a number of security threats related to browsing web are becoming a serious issue experienced by internet users such as phishing, adware, spyware, virus, spam (Obied and Alhajj, 2009). Vulnerabilities on websites and internet browsers features and settings can be exploited by these threats to steal or destroy sensitive information or track the online activities of users. A number of approaches and solutions have been proposed by many studies in order to improve security awareness about Internet and Web threats and make users browsing the internet safely.

A system called SmartNotes is proposed by Sharifi et al. (2011) which can help to make users aware of the potential threats when they browse websites. SmartNotes, which is a Chrome browser extension, allows the users are able to post comments and notes which could be used in rating and providing feedback about the websites and the related threats. In addition, questions and answers related to a specific website can be provided by the tool in Figure 3.8. Another feature is that the tool can calculate the scam percentage by collecting data about the current website from several sources. The tool tried to make the

user aware of the possible threat at the right time and this depends on the quality of the mutual cooperation between the users as it is a collaborative/community-based approach. In addition, the scope of the tool is limited by notifying the users about scam threats and only for Chrome browsers without providing them with awareness topics or materials related to the threat. Moreover, it has not been evaluated yet by the end-users in order to assess the functionality and usability of the tool. Another concern is that the tool does not offer any initiatives for monitoring the historical behaviour in order to evaluate the progress of the users in being safe online.

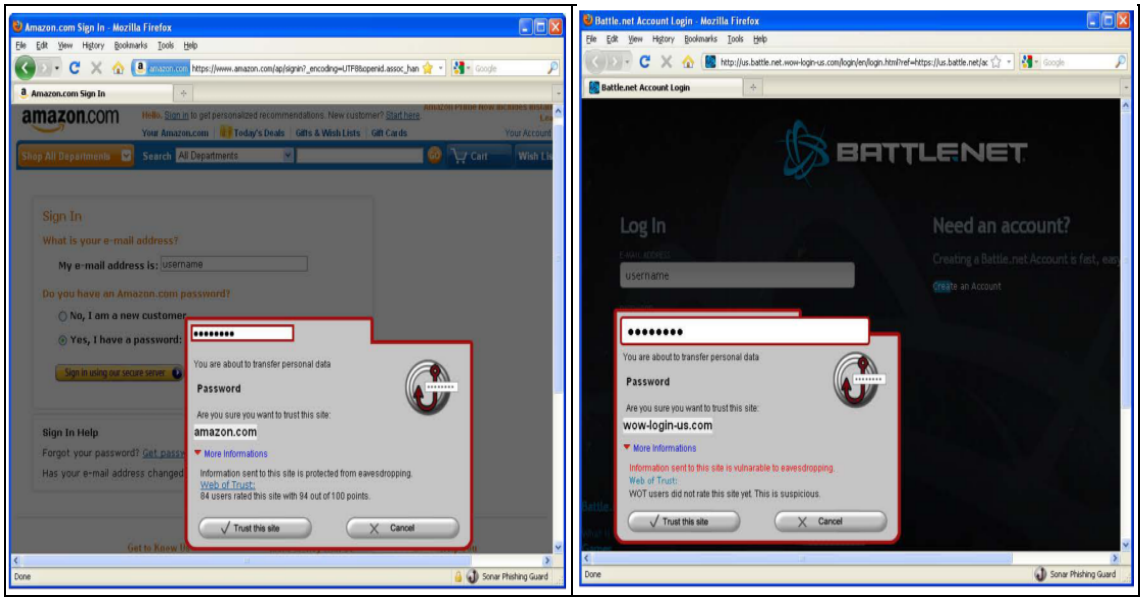


Source: (Sharifi et al. 2011)

Figure 3.8: Screenshot of the Smartnotes Browser Extension

Another Firefox plugin was proposed by Maurer et al. (2011) to raise cyber security awareness about phishing attacks and private data. Once the user enters one of the following critical data: credit card numbers, passwords or transaction authentication number (TAN), the tool will identify the type of the entered data by checking the HTML code for the password, using a specific algorithm to check the credit card numbers and finding input filed with 4 to 6 characters length with the word "TAN" to identify the

transaction authentication numbers. Next, an awareness dialogue will be displayed which includes: the critical data type that the user is entering, the correct website where the private data will be stored and 'More Information' option as shown in Figure 3.9. In the More Information option, the user is provided with an awareness message whether the current website is secure or not (phishing website). In addition, it includes a Web of Trust service to see how internet users are rating the website. Another option is that the user can add the website to the whitelist to avoid dialogue in the future. The tool has been evaluated in different case studies and the results showed the tool was acceptable by the participants and they were able to identify the phishing websites easily. The tool tried to draw the user's attention and make them aware when they deal online with confidential data at the appropriate time. However, the tool provides a limited awareness notification which deals only with three types of confidential data and phishing websites. In addition, there is a lack in monitoring the user online behaviour while using the tool such as generating a daily report which could make it difficult to evaluate the improvement in avoiding the phishing attacks.



Source: (Maurer et al. 2011)

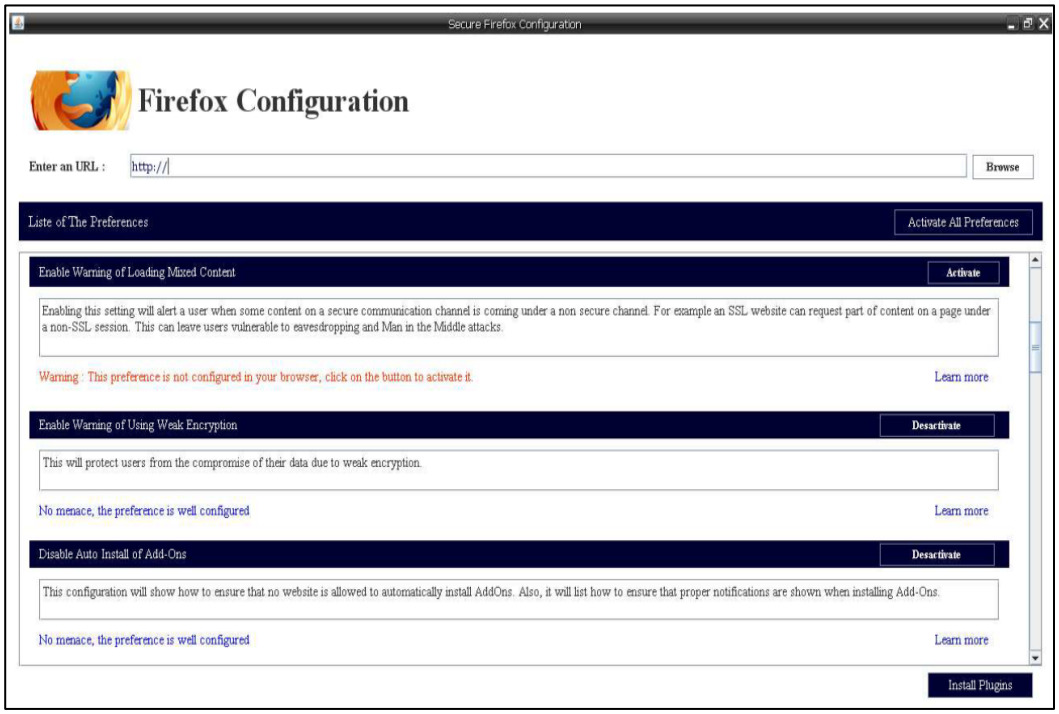
Figure 3.9: Screenshots of the Firefox Plugin Proposed by Maurer et al.

A theoretical approach was proposed by Jahankhani et al. (2012) to make internet users aware of fake and phishing websites. The proposed tool has three detection levels and each level has different process and techniques to detect fake websites:

- Level 1: URL is checked by analyzing the format of the URL whether it includes suspicious parts such as @, $ and dot. The user will be notified if the current website is legitimate or fake.
- Level 2: this level provides two stages of a check. Firstly, a black and white list of websites is created and gathered from common databases. Once the website URL is found in the blacklist, a warning message will be displayed to the user. Secondly, a warning notification: " page title and URL doesn't match – site may be suspicious" will be shown, once the tool checks and finds that there is no similarity between the webpage title and the URL.
- Level 3: this level is called Image-Based Screening which can collect the pixels information of the webpages in order to be stored and updated in a database. Next, the current webpage browsed will be captured and the pixel information will be checked and compared with the one stored in the database. Once the tool finds that they are similar, the user will be informed that the website is legitimate, otherwise the website is fake.

The tool intends to make the user aware in very limited scope which is the phishing websites. In addition, the tool flowchart is not designed effectively, For example, if the user passes level one successfully, they will be informed that the website is legitimate and it will not be checked by level two and three which might find that the website is fake in these two tests. In addition, the tool does not provide any type of historical behaviour for the users in order to check the user online behaviour.

Serrhini & Moussa (2013) claimed that many home users do not have appropriate knowledge in which security features should be enabled or disabled in browsers. Therefore, they developed a tool for home users called Automatic Safe Browser Launcher which can allow a user to surf the Internet securely. The tool has the ability to scan and detect all the installed web browsers. Once the user selects and clicks the preferred web browser, most of the required security setting features which are identified by the authors, such as updating web browser, network settings, encryption settings and javaScript settings, will be applied (enable or disable) in the selected browser before it is launched. All the preference reconfiguration for the browsers is applied in the Browser Preferences File or the Windows Key Registry. The user also can view all the misconfigured settings for each browser in the configuration page which has a description of each associated security risk and an activate button to enable each feature automatically as shown in Figure 3.10. it can also be connected to a security awareness platform to increase the user's knowledge.



Source: (Serrhini & Moussa, 2013)

Figure 3.10: Firefox Automatic Configuration Features

The browsers were tested with and without the automatic launcher in different scenarios. They found that when security features are configured more, the user will experience fewer internet vulnerabilities. The tool provides security protection and awareness for only the browsers Internet in Windows computers without supporting smartphones or other platforms. In addition, the tool provides does not provide the security configuration based on the current needs of the users, only one fixed reconfiguration list for all the users,which might not suit some users and restrict their online activities. This kind of enforcement might result in switching the tool off and using normal browsers to avoid the restriction. Moreover, the tool does not have an option which can motivate users.

A theoretical model was proposed by Potgieter et al. (2013) which aims to promote information security awareness based on behavioural activities when using a web browser. It called Targeted Awareness Browser Extension consists of four main components:

- Analysis Engine: it collects information from browser, web content and data storage in order to identify possible threats or required awareness.
- Event Engine: Once the collected data is received from the Analysis Engine, the Event Engine will decide if there is an event in the session which is required awareness.
- Awareness Content: it has the targeted awareness topics which could be essential for keeping users aware of the possible threats.
- Browser Extension Interface: it is responsible for displaying the awareness content to users and it will be designed as a vertical panel in the browser application.

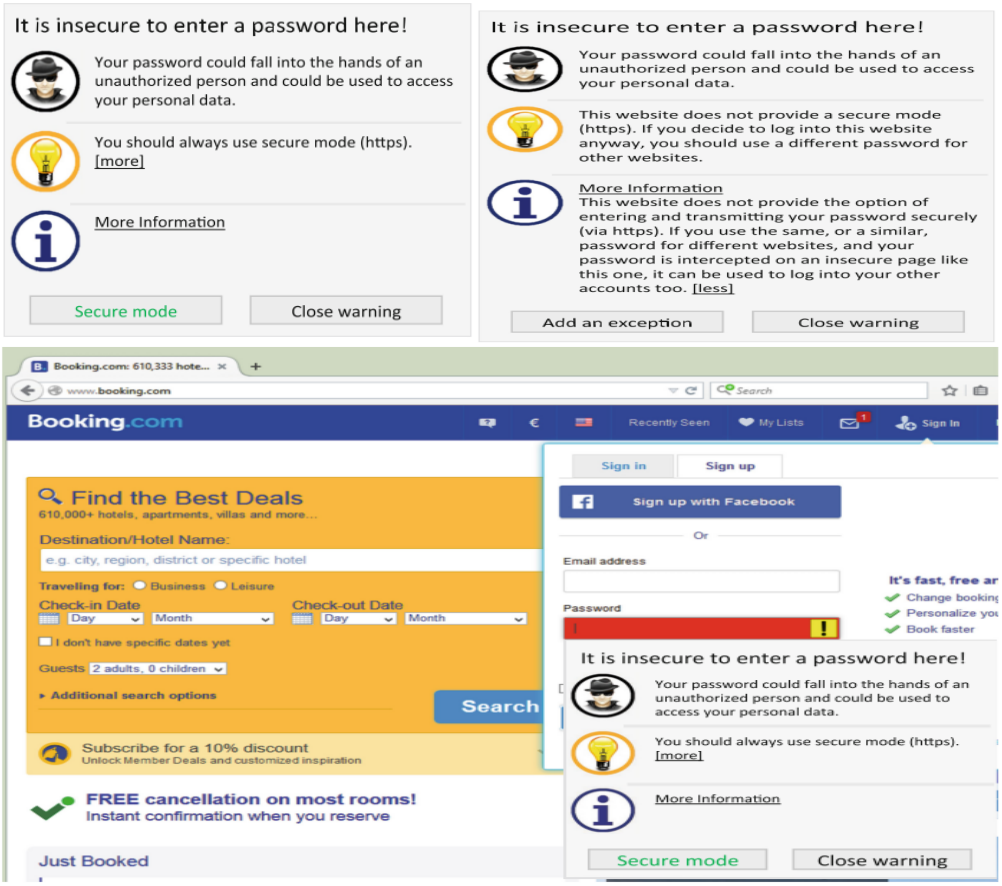
The tool plans to provide users with particular awareness when a possible threat might be experienced. For example, if a user is browsing a banking account, an awareness topic about phishing attacks will be shown to the user or awareness content about the risk of the malicious programs and attacks will be displayed if a user is browsing a website which has a malicious application or code. It seems that awareness topics are limited to the threats related to web browsing. In addition, the features of the historical behaviour and motivation are not mentioned in the tool which could affect the functionality of the tool and might lead to uninstall the extension from the browser.

Volkamer et al. (2015) developed a tool called PassSec which works as an add-on in Firefox browsers to provide security awareness about using passwords in unsafe websites. The first task of PassSec is to highlight all the password fields in different colours: green if the website is using HTTPS or red if it is using HTTP as shown in Figure 3.11.

Source: (Volkamer et al. 2015)

Figure 3.11: Highlighting of Password Fields To Draw Attention

The second task is to provide the users with an awareness dialogue when a password is typed in an unsafe website which is using HTTP. The dialogue has a warning headline: "it is insecure to enter a password". In addition, it contains a warning message about the possible result when typing the password insecurely: "Your password could fall into the hands of unauthorized persons and could be used to access your personal data". Moreover, PassSec can provide a secure mode which redirects the users to a secure connection (https) if it is available on the website as shown in Figure 3.12.

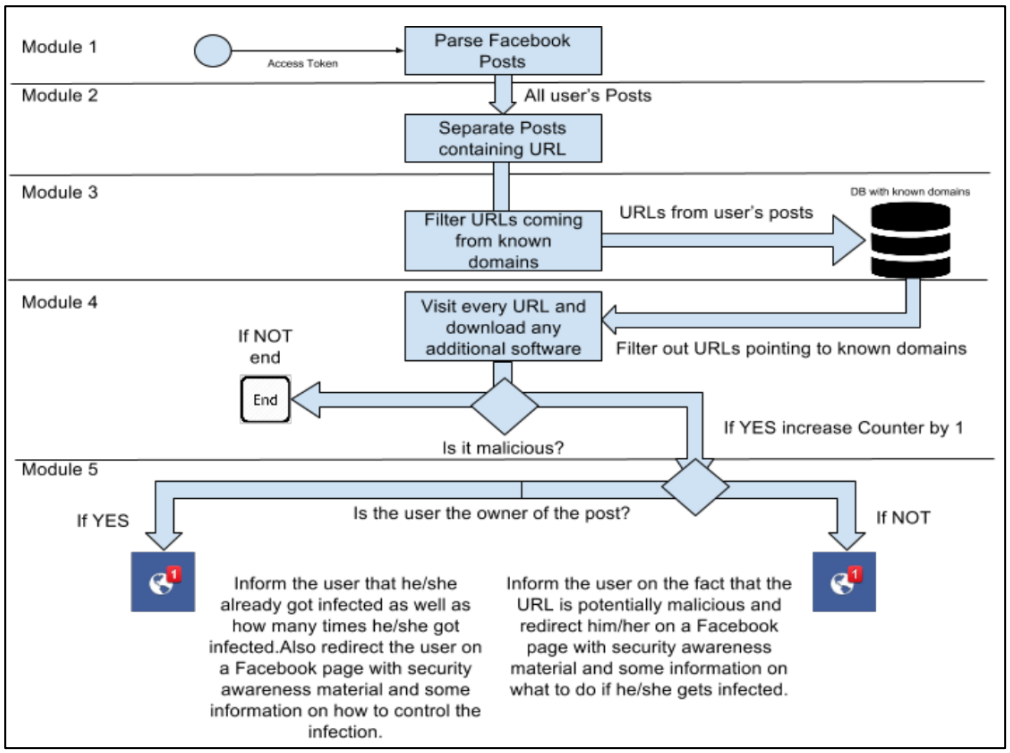


Source: (Volkamer et al. 2015)

Figure 3.12: Screenshots of PassSec

31 participants were involved in evaluating PassSec in different scenarios and aspects. The tool was successful to promote password security awareness. The attempts of the insecure logins were 476 times without installing PassSac while there were only 30 insecure login attempts when using PassSec. The usability aspects have been considered during all the model phases, the colours, icons, the options and the position of the dialogue box succeed to let the users pay attention to the awareness content. In addition, the tool was successful in providing the users with an awareness notification at the right time but it is very limited and only deals with password security in PCs and laptops. Furthermore, the tool has a lack of encouragement and behaviour analysis which could enhance the functionality further. For example, if the tool fond that the user browses safe websites and uses passwords securely, a digital score or certificate could be rewarded.

Another theoretical framework was proposed by Karavaras et al. (2016) which can provide awareness about the malicious links threats which might be experienced by social network users. The application called Soc-Aware has several modules in order to perform effectively as shown in Figure 3.13.



Source : (Karavaras et al. 2016)

Figure 3.13: Soc-Aware Application Framework

The first step is that an access token is received which provides permission for the application to access and analyse all user's Facebook posts. Secondly, posts which have URLs are identified and filtered based on the domain names such as youtube.com. Next, suspicious URLs which do not have well-known domain names are moved to module 4 in order to check the websites in each URLs in order to find a malicious code or software which could affect the users' security. Once a post is detected as a malicious URL, Soc-Aware will notify the user about how many times they experienced malicious actions and provide them with a Facebook page which includes security awareness materials and guidelines in order to mitigate the threats that they are experiencing. They stated that Soc-

Aware is currently under development and the main functions are being tested. Despite the fact that the tool is designed in order to make the user aware of the threat in the useful time, it is only applicable for Facebook users and only covers one threat which is malicious URLs. In addition, the application requires access permission in order to work which might be considered as a privacy threat.

3.2.4 Gamification

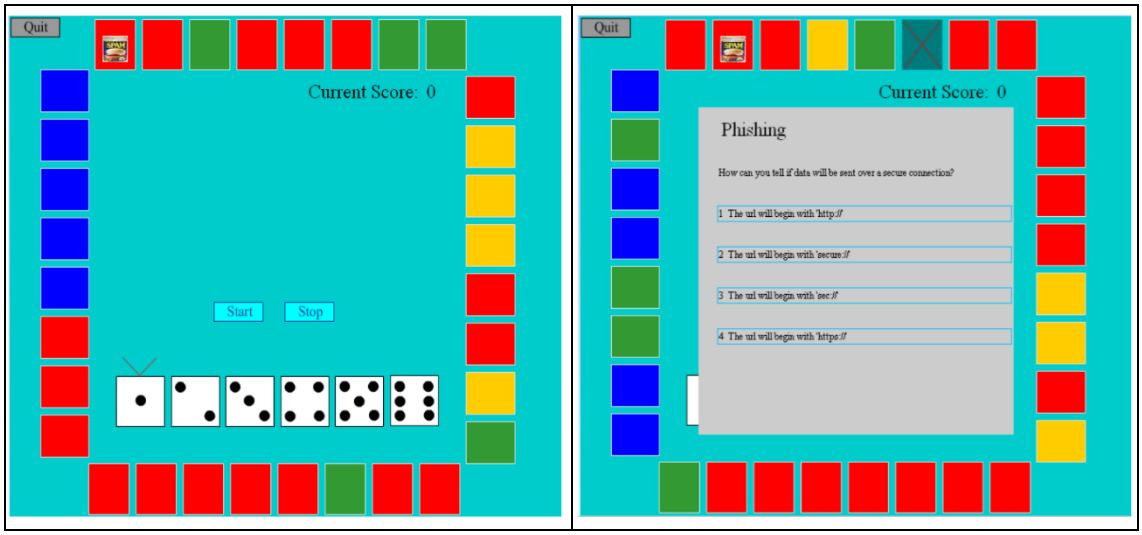
Another method to deliver the cyber security awareness content is to use the game platform which can be an effective approach for family members especially children and young people. Serious games or applied game are games which are designed and used for purposes other than entertainment (Susi et al., 2007). Gamification is considered as one of the common tools and techniques which are used to improve information security awareness and education. It is used as persuasive games that can influence and change user behaviour (König et al., 2019). Fogg (2002) proposed a number of persuasive technology principles which can be applied and used in designing gamification:

- Tunnelling: it is the procedures which are taken to produce a game experience which can include a chance for persuasion. Noticeable tangible results which can be seen can attract players to participate in tunnelling experience (Forget et al., 2009). Therefore, players should be taken through a sequence of events, stages and challenges in games.
- Conditioning: it has been argued that offering players rewards for their progress can encourage them to participate more in the game. It is kind of positive reinforcement, which can provide rewards for players when preferred behaviour or progress is achieved. There are many forms of reward system which are used in gamification applications such as a virtual gold star, badges and points.

- Suggestion: one of the persuasive technology principles is to offer messages and notifications at an appropriate time in order to make Gamification more effective. These notifications can be as a reminder in gamification to ask players to return to the game or carry out an activity or provide a hint for players when they are stuck with a challenge in the game.
- Self-monitoring: it has been stated in the persuasive technology principles that players can be encouraged to improve their performance by providing them with their progress regularly. Therefore, statistics that demonstrate players' scores and progress for their activity should be included in gamification.
- Surveillance: it is an important persuasive technology principle which enables gamification systems to review and analyse users' behaviour in order to reward users or find out their faults. In addition, when players know that their actions are monitored by others, they intend to participate in more certain actions.
- Tailoring: one of the persuasive technology principles is that relevant information in order to change their behaviour about a certain subject. Gamification should provide customised information in order to allow players to pay more attention to information.
- Reduction: it is recommended that gamification systems should facilitate tasks and make them easier and simpler by reducing some of the unnecessary steps.

Many serious games are proposed and designed to improve information security awareness and education. Newbould & Furnell (2009) proposed an online board game, called Play Safe, which provides awareness in four topics to mitigate the risk of social engineering attacks: phishing, advance fee fraud, spam and other attacks. The topics are distributed in 32 squares and each topic has a unique colour. At the beginning of the game, the user will use the virtual dice to select a square randomly. Next, the user will be

provided with a multiple-choice question. Then, a score, feedback and reference material will be offered based on the answer as shown in Figure 3.14.



Source: (Newbould & Furnell, 2009)

Figure 3.14: Screenshots of Play Safe Game

The game prototype was evaluated by 21 users; the vast majority of the participants stated that that they noticed an improvement in their knowledge about social engineering after playing the game. The game is designed to be played individually and it could be improved by allowing multi players or sharing the score with other players in order to be more motivated. In addition, the authors did not discuss how the awareness website will be shown in the game.

Arachchilage & Cole (2011) designed a mobile game for home users to educate them on how to avoid phishing attacks. The design consists of two parts: the game and the reference guide. Technology Threat Avoidance Theory (TTAT) was used to address the online issues which are required more attention from the users in order to mitigate the related online threats. The prototype provided links to an educational website as a reference guide. This game only taught users how to avoid only one type of the phishing attacks: the phishing website addresses (URLs) which make it very limited. In addition, the prototype has not been evaluated by the home users.

Another online game was designed by Labuschagne et al. (2011) which can enhance cyber security awareness in different aspects such as password security, social media security and phishing protection. Once the users answer all the questions of a specific section correctly, badges will be posted in the profile as a reward. They use social network sites as a platform to deliver the game in order to motivate the user to share it with friends and view each other's progression which could make a competitive atmosphere among the users and their friends. The user can view many materials and do quizzes which are related to each topic in order to move to the next level. However, again, the educational game was not evaluated by users and was limited in its coverage of security topics.

Yang et al. (2012) developed an Anti-phishing Education game which allows the users to learn anti-phishing knowledge while playing the game. In the game, each anti-phishing concept can include different scenarios and cases support. The game starts with a soldier John who needs to finish all the assigned missions without being infected by phishing attacks. During the game, the player has to identify if the current URL is a phishing attack or not. Scores and feedback are provided to the user immediately based on their progress. In addition, the players receive tips and assistance from John's commander which can help them to detect the phishing pages as shown in Figure 3.15. The game has been evaluated by 62 participants who have participated in a pre- and post-test about identifying the phishing pages. The results show that there has been a significant improvement in the participants' results after playing the anti-phishing game. In addition, the participants' satisfaction with the usefulness of the game is very good but there is negative feedback regarding the usability and the ease of use of the game which needs further improvement. In addition, the game has a lack of multiplayer features and sharing the results with others which can be a motivational factor. Furthermore, the scope of the awareness content of the game covers only the web phishing attack.

Source: (Yang et al. 2012)

Figure 3.15: A Screenshot of the Anti-Phishing Education Game

Another game based on e-learning platform was developed by Fruth et al. (2013) in order to make primary school children aware of online threats. The main game consists of three mini games which discuss the possible risk in online chatting, social networking and internet virus. Every part of the game was designed to simulate infantile learning environments in order to be attractive for children such as characters, metaphors and colours. A prototype test was conducted and evaluated by 30 children. It is true that the three mini games are designed in limited and basic content in order to suits the children aged between 7 and 9 years but the results show that virus and chat games do not have a good significant effect on the children's knowledge which needs to be improved.

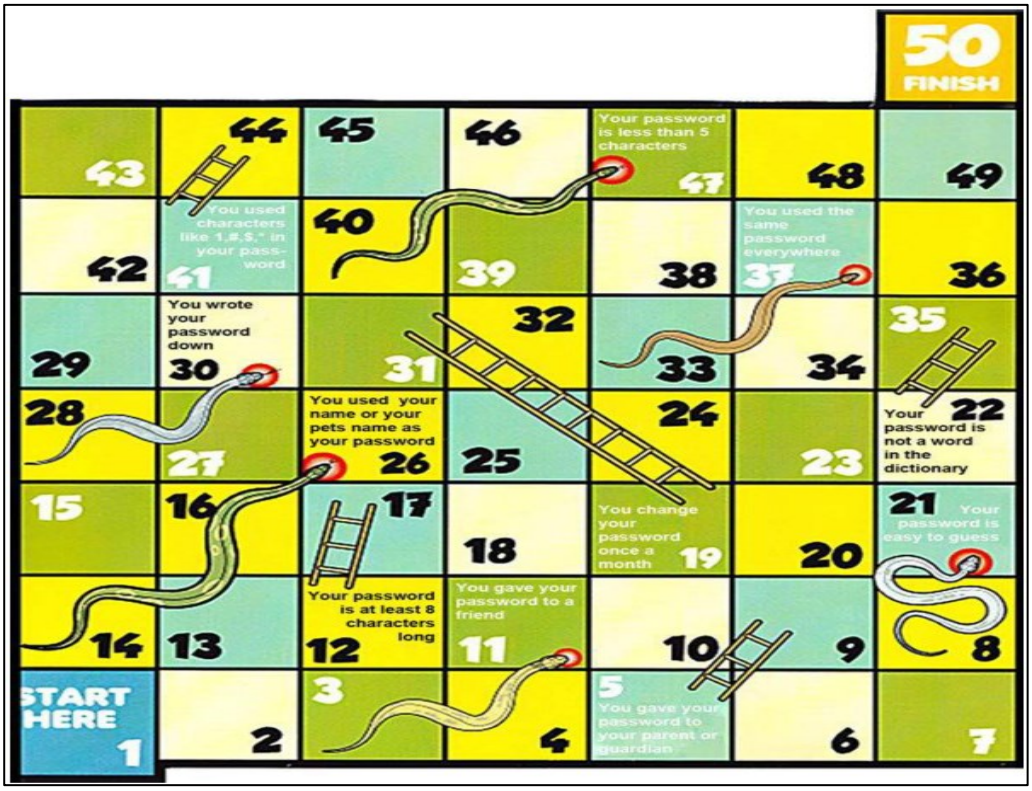
The majority of the current cyber security educational games provide awareness about only one single online threat or no more than two issues. As a result, an alternative game was designed by Juhari & Zin (2013) to cover different internet safety topics in four levels and each level has to be completed successfully to go the next level as a motivation factor:

- The first level: to avoid inappropriate website and popups.

- The second level: to keep the personal information protected.
- The third level: to behave safely on social network websites.
- The fourth level: to learn how to use email securely.

The game is tested and evaluated by 31 children given a pre-test and pro-test, the average result of the post-test after playing the game increases by 23%. In addition, the usability of the game in different aspects is evaluated with fulfilling feedback. The content of the game is designed for the children and does not support the rest of the family members.

The popular game "Snakes and ladders" was used by Reid & Van Niekerk (2014) in order to enhance the information security concepts and skills among children. The awareness contents were delivered to the children as Do and Do not lessons as shown in Figure 3.16. Several versions were designed in order to cover many information security topics such as password security, social network and virus security.



Source: (Reid & Van Niekerk, 2014)

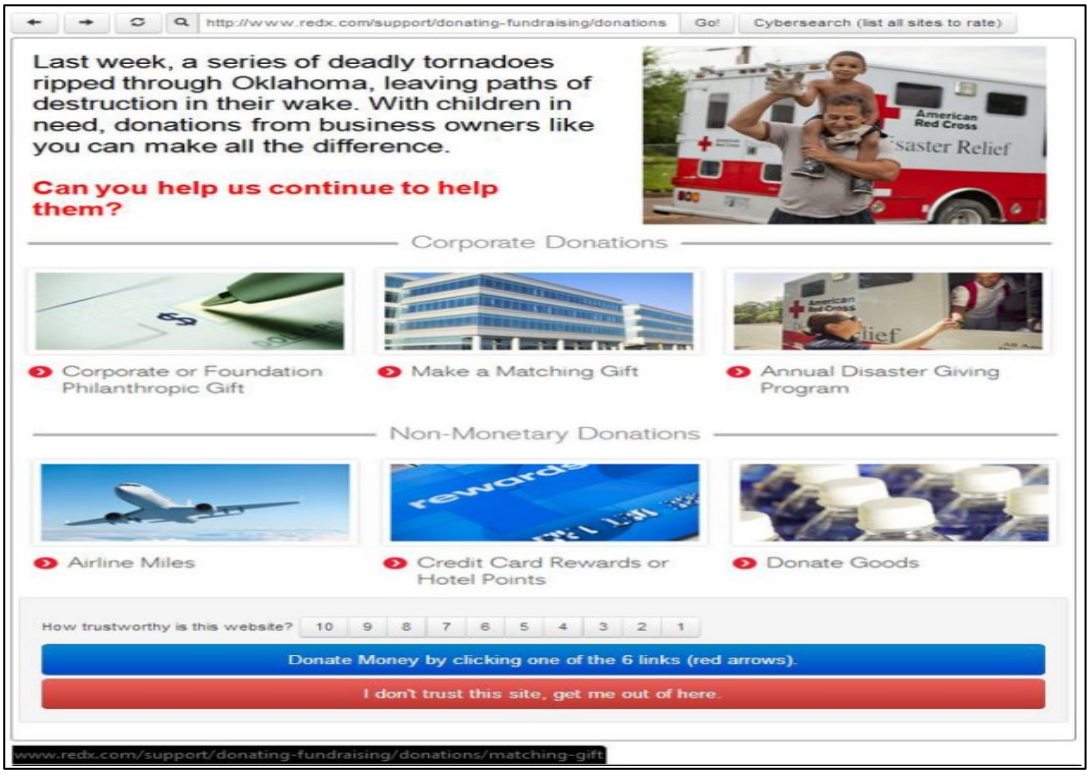
Figure 3.16: The Snakes and Ladders Password Board

Several experiments have been conducted in 2 schools and 3 different groups in order to evaluate the effectiveness of the game. The results show that around 54% of the participants knew not to write down their passwords before plying the game, the percentage increased to reach around 91% who knew this tip after playing the game. Although the game is entertaining as it must be played with a group of children, the content is limited to one type of awareness delivery method and one type of stakeholders.

Some of the users of social network websites are not fully aware of the related online security and privacy threats. Cetto et al (2014) designed a game to enhance privacy awareness among users of social network websites. The game called Friend Inspector accesses the player's Facebook account in order to retrieve the contacts and shared items such as pictures. The user is asked to select the most personal photo to him from two photos are brought from his Facebook profile. Next, the selected picture is presented with 20 profiles (user's friends and strangers), the user has to select the correct profiles who can view his shared pictures. At the end of the game, the user receives the overall score and recommendations to enhance their privacy settings. The game succeeded in making the user aware of the possible vulnerabilities which might be caused by the current implemented settings. However, the game requires access to a user's Facebook account which might be risky even though the authors claim that personal data is secured. In addition, the game prototype has not been evaluated by the main stakeholders.

Due to the increase in the number of online phishing attacks around the world, Hale et al. (2015) proposed an approach called CyberPhishing to utilize game-based techniques for online phishing awareness. The core idea of the tool is to simulate many types of phishing attacks in order to analyse the users' behaviour and actions which could help to identify the user's weakness and the required training in order to mitigate the possible risk. The

tool provides simulation modules for fishing attacks in three aspects: email, web browsing and social media. On the first page, users are provided with a story which contains a list of tasks which requires the user's decision. Once a user clicks one of the links, they will be directed to an interface related to one of the three aspects. All the contents are simulated and presented realistically in each interface. In addition, all the actions and usage are captured for analysis purposes. All the interfaces have an assessment scale in order to evaluate how the user trusts the presented scenario. Furthermore, users are provided with two options: trust the content by accepting and doing an action or distrust by ignoring or rejecting the action as shown in the web browsing simulation in Figure 3.17.



Source: (Hale et al., 2015)

Figure 3.17: Web Browsing Simulation Interface

Three phases have been planned to examine the effectiveness of CyberPhishing and how it presents the content realistically: Alpha test, Beta Test and Production. The alpha test,

which is phase 1, was conducted by 14 testers, the test results for the three mediums indicates that some contents need to be redesigned in order to make it difficult to be identified. In addition, comments and feedback have been received from the testers which could help to improve the tool in the next phases. CyberPhishing only tests whether the users have the ability to identify the phishing attack or not and it does not provide a particular cyber awareness when the users really need it. Furthermore, it does not have any awareness materials or topics which can be provided to the users based on the simulation results. Therefore, the tool should tailor the users to the required awareness material based on the result of the analysis behaviour. Moreover, the tool doesn't provide users with a score or certificate in order to motivate them.

From a different perspective, Lazarinis et al. (2015) designed a mobile application based on visual stories in order to attract children to learn about internet safety. The application only discusses three online issues related to children: Internet addiction, cyberbullying and sexual harassments. The feedback of the application evaluation is that children can understand the risk of internet addiction. The tool is designed with limited and basic topics in order to suits the elementary students but more learning topics and issues can be added and discussed in order to attract more groups of users.

Another educational mobile game, which is called CyberAware, was developed by Giannakas et al. (2015) which aims to allow children to learn about cyber security principles and online issues such as malware and spam while they are playing the game. In the beginning, children choose the required learning topic such as security or privacy, each topic consists of three stages. Each stage has to be completed successfully to go to the next stage in order to motivate the players. In the first game of the security learning topic, children have to identify basic cyber security technologies from different

technologies. In the second game, children are asked to link the security technologies (recognized in the first game) with the main function of each one. The third game aims to teach children how to deal with different online scenarios correctly by using suitable protection technology. For example, children receive the following scenario: "You received an email containing a music file. You should open and hear it", they should select the correct technology for this action such as antivirus, firewall, spam Filter or security updates. Once the players complete all the games successfully, they will be rewarded with CyberAware certificate as a motivation and satisfaction technique. The game has been evaluated by 43 participants in terms of user satisfaction, usability and effectiveness, 66.6 % did not experience any problem with the game, 85.2% would play the game at home, 47% recognized all 4 cybersecurity technologies compared to 32.6 % before playing the game. Only children from 9 to 11 years are the targeted group in this game. In addition, the game did not try to provide awareness materials based on the weaknesses of the users after completing all levels of the game.

Baslyman & Chiasson (2016) proposed a board game called "Smells Phishy?" which can enhance internet users' awareness about online phishing threats. The main idea of the game is that users need to behave safely and follow the cyber security best practice while they are shopping online in order to avoid phishing scams. The game includes several components such as board, cards (Task card, police card, hint card, credit card, shopping list) and movement tokens as shown in Figure 3.18. The player should purchase the required item from a specific store after passing the cyber security test described in the task card. A hint card can be purchased to help the user pass the security test successfully. There is a police card with each task card which could have a punishment or a prize for the player based on the task card result. In addition, the police card contains security advice and tips to mitigate online risks. 21 participants were involved in pre-tests and

post-tests to evaluate the effectiveness of the game. The result shows that the knowledge about online phishing safety has been improved among the participants after playing the game. Moreover, the majority of the players strongly agree that the game was fun and important to understand security. However, only the phishing attack is discussed in this game which makes limited. In addition the game cannot be played individually which might not be suitable for small families.

Source: (Baslyman & Chiasson, 2016)

Figure 3.18: Smells Phishy Game Components

3.3 Discussion

Many academic papers and articles have proposed several techniques and approaches which can have the ability to enhance the cyber security awareness among home users as presented in Table 3.1

Authors	Method	Bespoke Awareness	Usability Evaluation	Result
Tolnai & Von Solms (2009)	Portal	No	No	Not evaluated yet
Caceres & Teshigawara (2010)	Security Tool	No	No	A significant improvement in cyber awareness
Kritzinger and Von Solms (2010)	Security Tool	Yes	No	A theoretical design
Sharifi et al. (2011)	Browser Extension	Yes	No	The functionality of the tool has been tested successfully
Maurer et al. (2011)	Browser Extension	Yes	Yes	It improved the awareness of the home users
Arachchilage & Cole (2011)	Game	No	No	A prototype has been developed and tested successfully but no valuation by the home users
Labuschagne et al. (2011)	Game	No	No	The functionally and the effectiveness of the game has not been evaluated yet.
Labuschagne & Eloff (2012)	Security Tool	No	No	The functionally and the effectiveness of the tool has not been evaluated yet
Magaya & Clarke (2012)	Security Tool	Yes	Yes	It improved security awareness among home users
Jahankhani et al. (2012)	Security Tool	Yes	No	A theoretical design
Fruth et al. (2013)	Game	No	Yes	It improved learning about basic security threats among children
Juhari & Zin (2013)	Game	No	Yes	A significant increase in security knowledge
Smith et al. (2013)	Portal	No	No	It increased users' understanding of threats
Potgieter et al. (2013)	Browser Extension	Yes	No	It is only a theoretical model without designing a prototype
Cetto et al.(2014)	game	No	No	It has been used effectively to understand privacy settings on Social Networks
Volkamer et al. (2015)	Browser Extension	Yes	Yes	It significantly reduced the number of entering password on unsafe websites.
Rani & Goel (2015)	Security Tool	No	No	The system functionality has been tested successfully but not evaluated by the users
Hale et al. (2015)	Game	Yes	Yes	It improved users' awareness of different types of phishing attacks
Giannakas et al. (2015)	Game	No	Yes	It improved the children learning about cyber security
Karavaras et al. (2016)	Security Tool	Yes	No	It is only a theoretical model

Table 3.1: Studies Proposing Information Security Awareness Tools For Home Users

A number of studies have tried to provide the home users with awareness contents which are tailored to their needs in different aspects. Providing appropriate awareness content based on the level of cyber knowledge for the users was suggested by Kritzinger and Von Solms (2010). This approach might not be accurate due to the difference in the knowledge between the users. Another attempt was proposed by Magaya & Clarke (2012) to provide a bespoke recommendation and guideline based on the result of the risk assessment for the home users but the security controls are identified manually by the users which might be difficult for the novice users.

Other attempts have been done by researchers to provide a particular awareness when the users are browsing the internet. Sharifi et al. (2011), Maurer et al. (2011) Potgieter et al. (2013) proposed a browser extension to make the user aware of the phishing websites and the possible threats while surfing online, whereas Volkamer et al. (2015) designed a tool to show an awareness notification when the users are browsing insecure websites with password fields. While Karavaras et al. (2016) and Cetto et al. (2014) introduced approaches which can provide a tailored awareness for Facebook users. All these studies are proposed to work in a limited boundary and provide a limited content of cyber awareness which might make them less effective to cover most of the threats in different systems and applications. In addition, some of these approaches are proposed theoretically with no real evaluation of their functionality. Moreover, these approaches may display false alert which can make users confused with some requests.

Some studies such as Kritzinger and Von Solms (2010) Labuschagne & Eloff (2012) Serrhini & Moussa (2013) have tried to restrict home users' online activity and force them to apply security settings or to read awareness materials. This type of enforcement could create a level of undesirability which will result in the solution being switched off or

uninstalled. In addition, it has been suggested in some studies that cyber security awareness can be managed by the ISPs (Kritzinger and Von Solms, 2010, 2013). However, this is not a workable solution because of many issues such as technical, privacy, financial and legal issues. The functionality of this approach can become more complicated if there are multiple technologies which are working on multiple ISPs. The motivation for this suggestion is that the authors want to give this responsibility to someone who is better able to manage it. This idea might manifest itself more properly within the family situation. There is an individual responsibility of information security within the family unit which might be improved when it is handled and managed by a member of a family who is at least more interested in information security and technologies. In addition, novice users can be given some responsibilities in order to improve their security and technical skills.

An example of a worse scenario can easily happen at any time is that if a home router is compromised because of known vulnerabilities such as using weak or a default password or venerable OS, an attacker can exploit these vulnerabilities to attack the connected devices in the same network. This kind of risk can be mitigated by having an oversight of the technologies in terms of what is being used and what is being protected in a holistic manner by implementing some form of policy in order to understand the expectations of what they want to achieve, similar to the approach which has already implemented in organisations.

The vast majority of the educational games are dedicated to a single area, limited scope and they do not successfully adapt to the multi-threat, multi-technologies and services. They have not tried to provide tailor-made awareness content based on the present needs of the users. In addition, they are designed to offer cyber awareness for children without

providing valuable awareness for the rest of the family members.

As most of the tools are optional to be used and their main stakeholder is the home users, it is important to encourage and motivate the users to be engaged with the tool in order to promote the cyber knowledge and awareness. The majority of the tools have not introduced any kind of motivations such as scores or virtual badges. For example, it can be easily introduced virtual badges or a cyber hero of the week in the family unit which could help to create a motivational environment between the family members. This can help in encouraging users to participate more in systems as suggested by the persuasive technology principles.

The concept of classifying users into three different levels: novice, intermediate and advanced have been used in several studies and approaches such as Kritzinger and Von Solms (2010) and Arachchilage and Cole (2011). This can help in providing security awareness based on the level of users in order to improve their awareness effectively. Users can be asked different questions about technologies and cyber security in order to identify their current level. The level of users should be reviewed frequently in order to check which users need to be upgraded to the next level or downgraded.

Users should be prepared very well to stay safe online. Informing users about different types of online threats is not enough to keep them protected. They should have the ability to know what they can do to be protected from the online threats and how to configure and manage their security controls and safeguards properly. This suggests that the current security awareness approach should be improved and changed from only telling users about different security threats and issues to improve their ability to manage different controls and mitigate different threats (Kritzinger and Von Solms, 2010; Furnell and Clarke, 2012; Furnell and Moore, 2014).

Several studies indicate that there is a need for an approach that can provide the users with bespoke awareness information which can enhance the security practice among home users (LaRose, Rifon and Enbody, 2008; Davinson and Sillence, 2010). Howe et al (2012) argued that there is a current need to integrate all the security activities and configurations in a comprehensive tool which can improve information security and reduce the heavy load on home users in managing different security tools and settings for different threats.

Another recent study was conducted by Nthala et al. (2018) revealed that there is a clear need to develop a usable tool can be used by non-experts to manage the security configurations for different devices and services at home which could motivate home users for better security and simplify the task for them. In the same context, Rao and Pati (2012) identified in their study that there is a current need to develop a usable tool for awareness and security controls management based on users' knowledge and behavioural pattern which could improve home users' perception of information security.

From the prior discussion, it is clear that there is a need for a bespoke individualized personalized approach that takes into account knowledge and awareness of the technologies, applications and services that users use and provides bespoke information directly based upon the current security posture. In order to measure and understand how the home users are doing something, well or badly? , it needs to be defined against something by using security policy in order to deliver customized awareness contents. Despite the fact that many approaches and tools have been proposed for the home users to promote cyber security, they are providing general, static and limited awareness content. Therefore, there is a need to provide the users with some kinds of policies which can deliver customized awareness content.

3.4 Summary

Despite the fact that the above analysis of the literature review shows that many approaches and tools have been proposed for the home users to promote cybersecurity, there is a lack of providing a tailored security awareness based on the users' needs. These leaves users open to a variety of attacks that would compromise their information, systems and networks. Accordingly, it is clear that there is a need for a usable, educational bespoke individualized approach which can configure, manage and monitor information security across devices and technologies and services within the home by taking into account user's knowledge, skills, current needs in an adaptive and usable manner in order to raise cyber security awareness. The next chapter discusses the research methodology which will be used and applied in the stages of this research in order to achieve the aims of the research.

Chapter Four

Research Methodology

4 Research Methodology

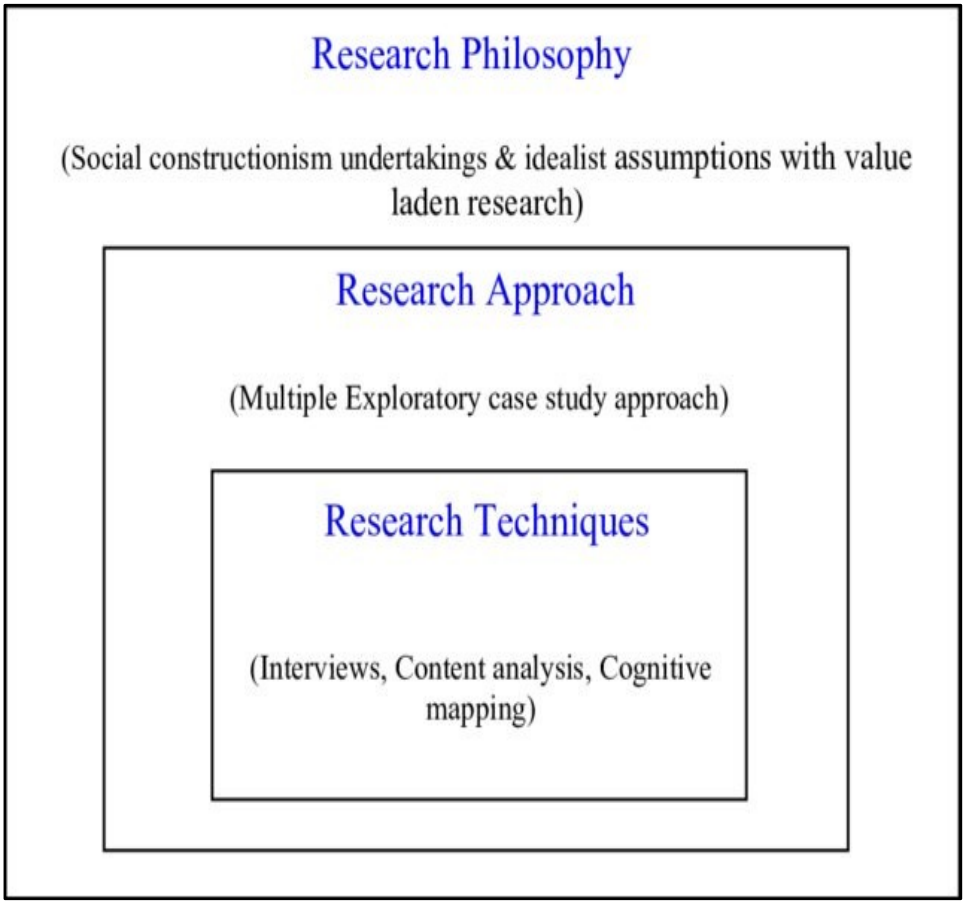
4.1 Introduction

Selecting the appropriate research methodology is very important in order to gather correct data which can help in achieving the main objectives of the research study (Burgoyne and Cooper, 1975). Robson (2002) introduces four areas which can be the motivational reason for conducting research summarised by Runeson et al. (2012) as:

- Exploratory study focuses on discovering what is going on, looking for new visions and making ideas and assumptions for a new study.
- Descriptive study focuses on describing an event, case or incident.
- Explanatory study focuses on looking for a clarification of a problem or an incident.
- Improving study focuses on improving a certain specific part in the studied event.

As the main goal of this research is to improve security management and awareness for home users, the improving approach is mainly employed in this research. In addition, exploratory and explanatory are used for exploring and investigating the current gap and lack of information security management and awareness for home users. Also, the descriptive approach is employed for describing the previous works for improving security management and awareness for large organisations, small businesses and home.

The research methodology is a systematic approach which can be used to find solutions for problems, answers for questions or gain more knowledge. Rajasekar et al. (2013) define research methodology as "The procedures by which researchers go about their work of describing and predicting phenomena". Kagioglou et al. (1998) state that the research method can be divided into three elements research philosophy, research approach and research techniques as showing in Figure 4.1.



Source: (Kagioglou et al, 1998)

Figure 4.1: A Nested Approach for Research Method

The purpose of this chapter is to discuss different research methodologies, philosophies, paradigms, approaches, strategies and methods used in this research.

4.2 Research Philosophies and Paradigms

There are different methods and approaches can be used in conducting research. Selecting a particular approach or method is mainly related to the philosophy of research. Research philosophy is defined as a belief about the approach for collecting, analyzing and using data about particular event or case (Lehaney and Vinten, 1994). Research philosophy has an impact on selecting the methodologies used in research. Analysis methods and data collection procedures can be influenced by research philosophy which is used in a particular study (Crossan, 2003). Johnson and Onwuegbuzie (2004) and Creswell (2016)

argued that research methodology and methods should be selected based on the research question and the research problem which is investigated by the study.

Lincoln et al. (1985) Guba and Lincoln (1994) and Vaishnavi and Kuechler (2007) argue several fundamental philosophical assumptions should be included in any research:

- **Ontology:** focus on the nature of reality.
- **Epistemology:** focus on how reality or knowledge can be known or explored.
- **Methodology:** focus on the methods used to discover reality or gain knowledge.
- **Axiology:** focus on the values are being held by individuals or groups.

Four qualitative research paradigms are suggested by Guba and Lincoln (1994): positivism, post-positivism, critical theory and constructivism. The design since was added as an approach based on interpretivism (Vaishnavi and Kuechler, 2007). In addition, three groups related to epistemology were introduced by Orlikowski and Baroudi (1991): positivist, postpositivist (critical) and antipositivism (interpretive).

In research, each paradigm has a fundamental philosophical stance. Fontenele (2017) introduces a summary in Table 4.1 for the characteristics of major research paradigms and design science which includes ideas from Lincoln et al. (1985), Orlikowski and Baroudi (1991), Gable (1994), Vaishnavi and Kuechler (2007), Harris (2011) and Weber (2010).

Stance	Positivism	Postpositivism (Critical)	Interpretivism (Antipositivism)	Design Science Research
Ontological	Realism (single reality, knowable, probabilistic)	Critical realism	Relativism, multiple realities, socially constructed	Multiple realism, socio-technologically enabled
Epistemological	Objectivist, dualist, empirical testability of theories	Objectivist, modified dualist	Subjectivist, transactional (knowledge emerges from interaction)	Knowing through making, iteration reveals meaning, improving the world through intervention
Methodological	Quantitative (statistical)	Quantitative and qualitative	Qualitative (participation, hermeneutical)	Qualitative exploration and quantitative confirmations
Purpose	Prediction/ control, explanation / verification	Generalisation, falsification	Transfer of findings	Developmental (measure artefactual impacts on the system)

Source: (Fontenele, 2017)

Table 4.1: Characteristics of Major Research Paradigms and Design Science

Positivism can be considered as a common research paradigm used in the researches (Orlikowski and Baroudi, 1991; Harris, 2011). Collis and Hussey (2003) defined positivistic philosophy as "approaches that are founded on a belief that the study of human behaviour should be conducted in the same way as studies conducted in the natural science". This paradigm studies only observable phenomena and it depends on reasons and observations as a tool for understanding, studying and analysing human behaviour (Henderson, 2011). Therefore, the methods which are used to collect data in positivist researches are experiments and observations (Mingers, 2004). Avison and Elliot (2006) argued that the positivist paradigm deals with testing hypotheses, operational or measurable procedures dependent and independent variables which are used to examine proposals and suggestions in order to deliver a good conclusion.

Interpretivists are also known as antipositivists or phenomenological philosophies which aim to discover the real value of social experience (Katadae, 2000; Harris, 2011).

Phenomenological philosophy is defined by Titchen and Hobson (2005) as "the study of lived human phenomena within the everyday social contexts in which the phenomena occur from the perspective of those who experience them". A holistic view can be accepted by Interpretivists when they recognize several realities (Ousmanou, 2007). These realities can be gained and achieved only through social constructions such as language, consciousness and shared meaning (Myers, 1997). Therefore, interpretive research can be generally considered subjective which is opposed to positivism which deals with objective researches (Harris, 2011).

The critical realism paradigm works with social reality and used as a philosophical framework for social science. this paradigm includes two different viewpoints: postmodern scholarship and critical theory (Mingers et al., 2013). Mingers and Willcocks (2014) argued that the critical paradigm the ontological reality of a variety of different entities. It is not required that these entities need to be measurable, or observable while they can be hypothesised and they have causal effects. In critical realism researches, views and opinions can be collected from participants in a subject or a situation which is being investigated or studied. In addition, the experience and the background of the participants can be studied and recognised in order to assess their impact on any study (Creswell, 2003). The difference between a positivist approach and critical realist approach that positivism uses experiments and observations to make the final decision in research. However, critical realism focuses on dealing with several restrictions which can be faced during different phases of the research. In this paradigm, qualitative methods are the most popular techniques which are used for collecting data and doing further analysis. Nevertheless, mixed methods which include qualitative and quantitative techniques can be used in some critical realist approaches (Neuman, 2000).

Design science research is considered as a new approach in the field of research (Reubens, 2016). It helps to improve the current situation through intervention and constructing a new reality such as solving problems (Iivari and J. R. Venable, 2009). Aken (2004) states that design science research tries to design solutions by developing reliable knowledge. Both qualitative and quantitative methods can be used to collect valid data and knowledge in design science research. The next section provides more information and explanations about design science research.

4.3 Design Science Research and Action Research

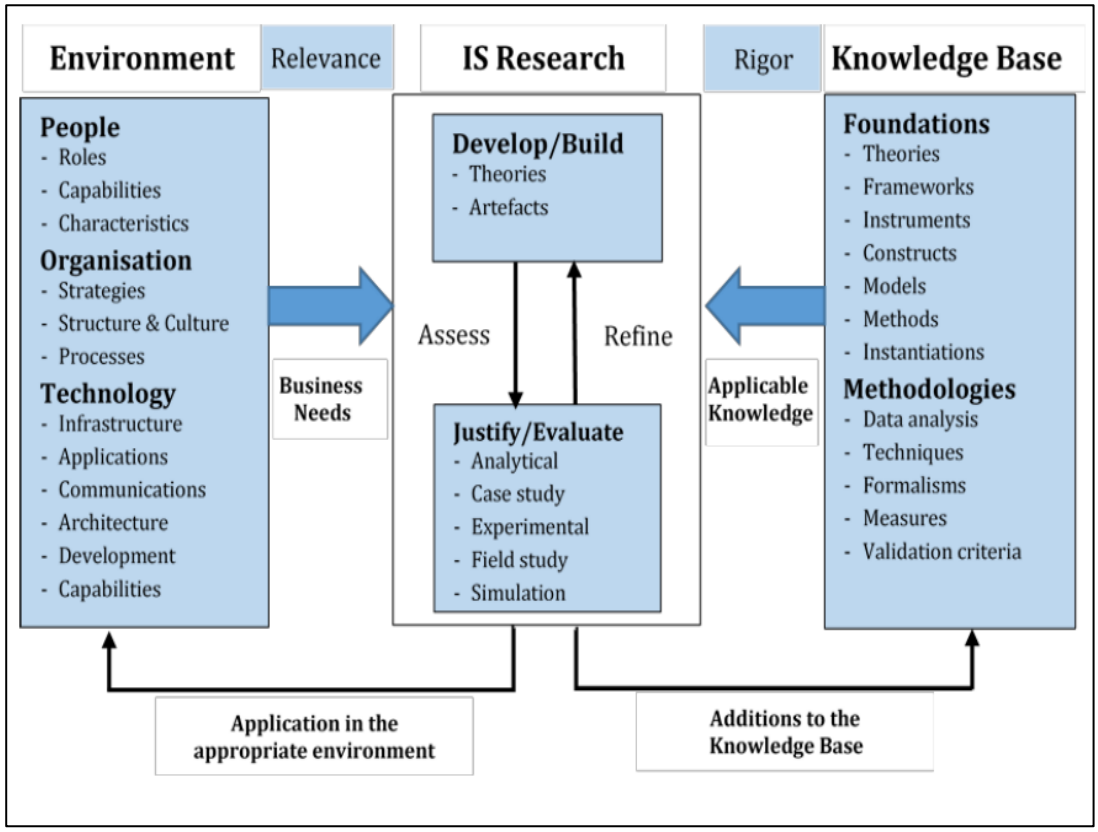
Design science research (DSR) is a research methodology used to conduct information and communication technology research (ICT). Design science research is used in producing long-term problem-solving methods and techniques in order to achieve the main objectives through innovation (Gregor and Hevner, 2013). The DSR is defined by Hevner and Chatterjee (2010) as "A research paradigm in which a designer answers questions relevant to human problems via the creation of innovative artefacts, thereby contributing new knowledge to the body of scientific evidence. The designed artefacts are both useful and fundamental in understanding that problem". Design science research is used in the information systems field for creating and building several socio-technical artefacts and products such as artificial intelligence techniques, decision support systems, management information systems and modelling tools (Hevner et al., 2004). An extensive analysis can be conducted under the framework of the design science research which can help to identify practices, ideas and thoughts which can be included in the research process (Kuechler and Vaishnavi, 2012).

The application of the design science methodology has been used in many types of research and studies in the domain of information security. Dennis et al (2014) developed

and evaluated a national cyber-security framework for Jamaica (JNCF) by applying the design science approach in all the stages of the research. Alqahtani (2017) explored the implementation of ISPs to evaluate policy suitability and to determine user awareness and compliance with security policies. Nykänen and Kärkkäinen (2018) used design science research to develop and evaluate novel knowledge interface system for information and cyber security risk management. The author indicates that a design science approach could help develop a more appropriate format for ISP that is useful and easy to use. In addition, Proença and Borbinha (2018) presented a maturity model for the planning, implementation, monitoring and improvement of an Information Security Management System based on ISO/IEC 27001. The authors applied design science research methodology in their research as they stated that it is appropriate for the development of maturity models.

Hevner et al. (2004) proposed a conceptual framework for implementing and evaluating information system researches as illustrated in Figure 4.2. The environment in the proposed framework specifies the boundary of the problem which includes three elements: people, originations and technologies. The framework tries to include two dimensions of paradigms: behavioural science and design science in order to easily compare between them. Business needs are identified, assessed and evaluated based on the organisation's goals, the current infrastructure and process. research in the information systems field includes two stages: behavioural science and design science. Behavioural science deals with research by developing and justifying theories that identify, clarify or predict situations which can support to achieve the business need. While design science deals with research by building and evaluating the designed artefacts which can help to achieve the current need. Knowledge base component in the proposed framework consists of foundations and methodologies. Foundations include

different elements used in the develop/build stage such as theories, frameworks, instruments, methods. Methodologies offer guidelines including techniques, measures and criteria which can be used in justify/evaluate stage. Once the appropriate methodologies and foundations are applied in the research study, rigour can be achieved in order to ensure the innovation of the research study which can help to meet the business needs.



Source: (Hevner et al., 2004)

Figure 4.2: Information Systems Research Framework

Hevner et al. (2004) proposed seven guidelines which can be used in design science research. The guidelines are provided in Table 4.2 to build an efficient design science research by giving a better understanding of the requirements. Guideline 1 relates to design as an artefact and seeks to produce a feasible artefact by using design science research which can be applied in different forms: a construct, a model, a method, or an instantiation (Hevner et al., 2004). Guideline 2 discusses problem relevance in research

study and defines the objectives of the design science research which can help to develop effective technology based solutions for the current problems.

Guideline	Description
Guideline 1: Design as an Artefact	Design-science research must produce a viable artefact in the form of a construct, a model, a method, or an instantiation.
Guideline 2: Problem Relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.
Guideline 3: Design Evaluation	The utility, quality, and efficacy of a design artefact must be rigorously demonstrated via well-executed evaluation methods
Guideline 4: Research Contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artefact, design foundations, and/or design methodologies.
Guideline 5: Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artefact.
Guideline 6: Design as a Search Process	The search for an effective artefact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.
Guideline 7: Communication of Research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

Source: (Hevner et al., 2004)

Table 4.2: Guidelines for Design Science Research

Design evaluation is discussed in guideline 3 which states that rigorous well-executed evaluation methods must be used to validate the utility, quality, and efficacy of a design

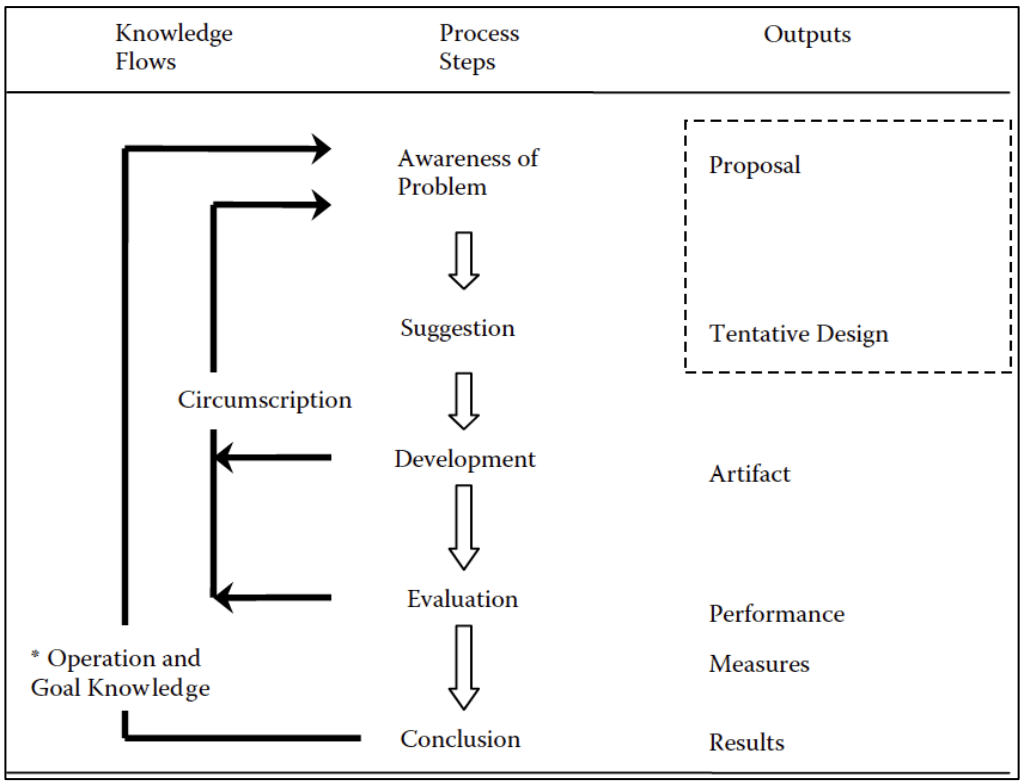
artefact (Hevner et al., 2004). Guideline 4 is concerned with research contributions which must be clear and variable when designing artefact, foundations and methodologies in order to provide an effective design science research. Guideline 5 states that rigorous methods should be applied during constructing and evaluating the design artefact.

Guideline 6 states that a good search process should be designed which can be done by employing the available methods in order to produce an effective artefact. Finally, guideline 7 discusses the communication of research and states the design science must be efficiently introduced to the management and technical spectators.

Vaishnavi and Kuechler (2007) outlined the process of design science research methodology. They argued that a number of steps should be considered in research which uses design science research methodology, the steps are listed below as illustrated in Figure 4.3:

- **Awareness of Problem:** awareness of an interesting problem which can be found in industry or a reference discipline. A proposal for new research can be delivered from this phase.
- **Suggestion:** it is a creative process for envisioning a new functionality based on novel configurations of new or current elements. A tentative design is the output of the suggestion phase.
- **Development:** the process of developing and implementing the tentative design is completed in this stage. An artefact is the output of the development phase.
- **Evaluation:** in this stage, the evaluation of the artefact can be done in stage by considering the criteria which can be stated in the proposal in the first stage in order to measure the performance.

- **Conclusion:** this is the final stage in a specific research effort. The results are consolidated, written up and judged good enough.



Source: (Vaishnavi and Kuechler, 2007)

Figure 4.3: The General Methodology of Design Science Research

Action Research (AR) is another philosophy and methodology which is generally applied in social sciences. Rapoport (1970) defines action research as "*action research aims to contribute both to the practical concerns of people in an immediate problematic situation and to the goals of social science by joint collaboration within a mutually acceptable ethical framework*". Bryman and Bell (2011) argued that the researcher and the client in the action research can work together in diagnosing and analysing the problem and in proposing and developing a solution based on the result of the analysis. Susman (1983) proposed five phases which can be conducted by using action research methodology starting from diagnosing the problem until identifying the general finding as shown in Figure 4.4.

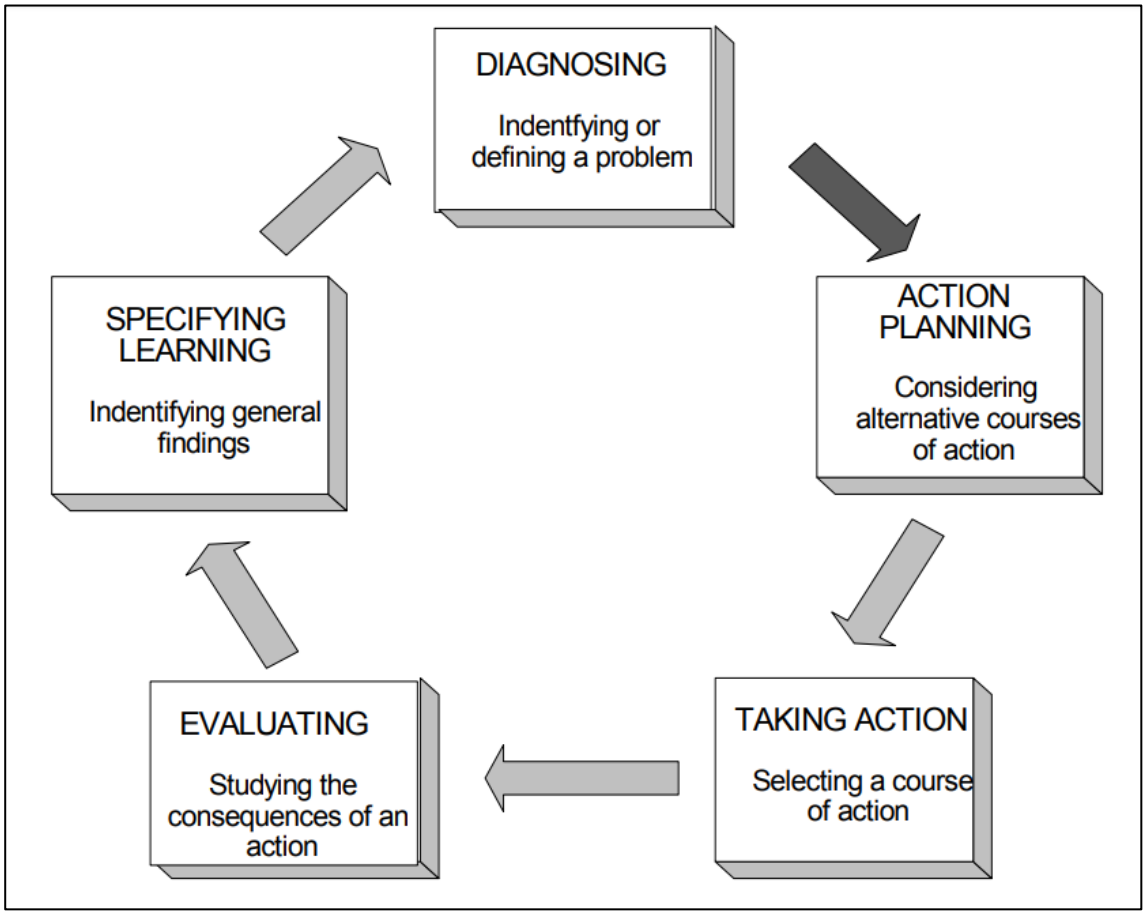
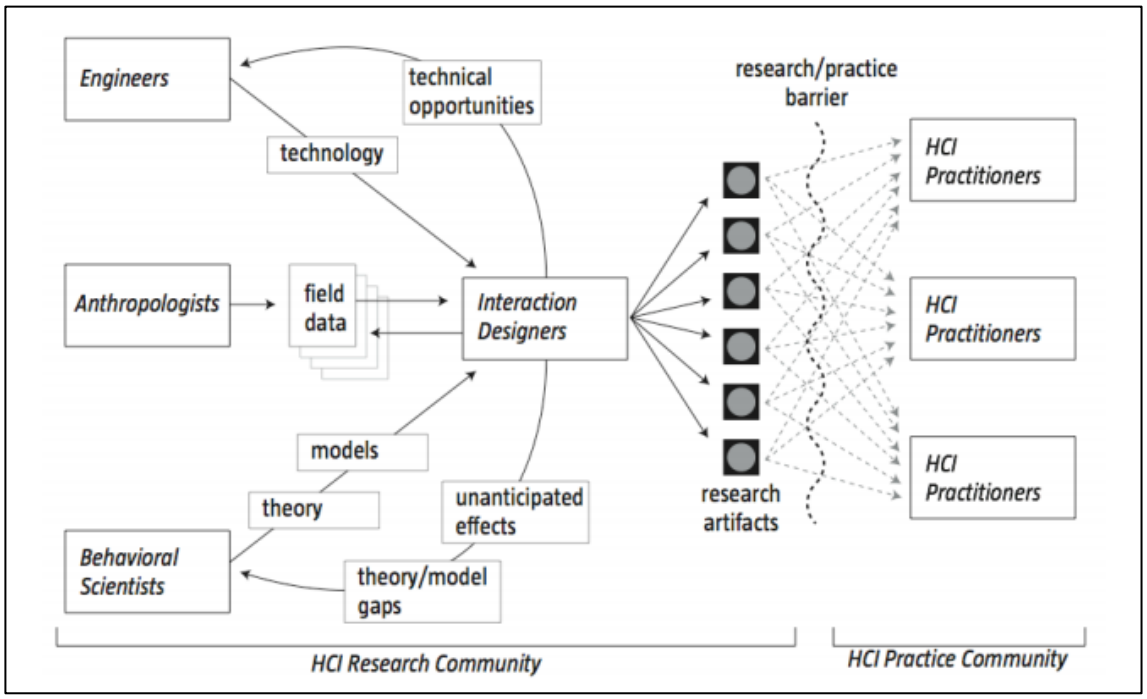


Figure 4.4: Detailed Action Research Model (Adapted from Susman, 1983)

While the design science research methodology might help in designing and developing an artefact without the presence of a client, the action research methodology is generally repeated processes during the investigation and the analysis between the researcher and the client which might not participate in a technology artefact (Iivari and Venable, 2009). it has been argued by Kappen (2019) that the client in action research is usually large organisations or institutions that are looking for improving their strategies, work environment, practice and knowledge base in their systems. The design science research methodology is often used for creating, designing and analysing novel artefacts which can be used to extend human and organizational capacities (Hevner *et al.*, 2004; Vaishnavi and Kuechler, 2007).

Zimmerman et al. (2007) found that the HCI community have experienced some difficulties in integrating design in research. Therefore, they proposed a model for interaction design research in HCI which allows design researchers to collaborate with HCI engineering researcher and behavioural science researchers in order to produce a good research artefact. Figure 4.5 presents the components of the proposed model and the interactions between them.



Source: (Vaishnavi and Kuechler, 2007)

Figure 4.5: A Model for Interaction Design Research in HCI

4.4 Research Methods

It is important to select the appropriate research approach in order to reach a satisfactory result and achieve the goals of the study (Creswell, 2016). There are two main research approaches: quantitative and qualitative. Each approach uses different research methodologies and related to a specific research philosophy. The quantitative approach usually is used with postpositivist philosophy while the qualitative approach is usually

applied with interpretivist philosophy. Both approaches have a number of advantages and disadvantages.

The quantitative approach focuses on collecting quantifiable data in order to be analyzed by statistical tools easily during the analysis process (Bryman and Bell, 2011). The associations between variables can be measured and analyzed by using numerical data in a quantitative approach. The analysis of a quantitative approach is repeatable very easy and simple because the analysis process and procedures are constant and specified (Parker, 1998). Quantitative research approaches use structured techniques such as questionnaires to collect data in order to test hypotheses or explain and define an event (Bernard, 2000; Allwood, 2012). Quantitative methods have been applied in the field of information security in many studies. For example, Alarifi et al. (2012) and Aloul (2010) both used questionnaires to evaluate cyber security awareness in different countries.

The qualitative research approach focuses on gathering data which is unquantifiable. The collected data in qualitative research is usually subjective and deep. The process objectivity can be affected in qualitative research as the researcher is usually involved in the process of the research (Bernard, 2000). Unstructured tools such as interviews, focus groups and observations are usually used for collecting data in qualitative studies to be used for exploring phenomena or developing a theory (Bernard, 2000). A qualitative approach has been used in many studies and researches in the information security domain. For example, Furnell et al. (2008) conducted a qualitative study by interviewing novice users to assess their information security awareness and online experience.

Another method called mixed methods, combining quantitative and qualitative methods (hybrid approach). The main goal of the mixed methods research is to increase the advantages of qualitative and qualitative research and to reduce the disadvantages and

drawbacks of using the mono method (Gelo et al., 2008). Creswell and Clark (2011) stated that mixed methods research can help to answer the research questions by collecting evidence and data from different sources and participations. Toomela (2008) explained that better integration between the data collection and the analysis can be achieved by employing the mixed methods research, compared to the research which uses one methodology. In addition, mixed methods research can help in validating the findings and reducing alternative descriptions and explanations for the findings (Johnson and Turner, 2003). Furthermore, correct and complete findings can be collected by using mixed methods (Coyle and Williams, 2000). Moreover, Morse and Chung (2003) argued that a better-balanced view can be achieved by employing mixed methods research, compared to the mono research which uses only one method (quantitative or qualitative).

4.5 Data Collection Techniques

Using the appropriate data collection technique is important in order to get accurate data which can help in answering the research questions. There are several types of techniques used in research based on the research objectives and used methods such as interviews, focus group, questionnaires and observation and case studies.

4.5.1 Questionnaires

A questionnaire is a common method used to collect data by gathering answers from individuals for a number of questions and each participant is required to answer the same questions which are already arranged beforehand (Saunders et al., 2009). There are many advantages of employing a questionnaire method in data collection in research. First of all, the questionnaire is one of the most used techniques in quantitative researches which will help to collect quantifiable and numerical data which can be imported to statistical tools in order to get more analysis (Bryman and Bell, 2011). The second reason is that the

researcher can be able to collect data from a large number of participants based on the nature of the research. Also, the participants can provide true answers and responses as they are not affected by the existence of the researcher (Dillman, 2011). Furthermore, participants can answer the questionnaires at their convenient time. Moreover, the online questionnaires can be easily distributed and managed by using several methods such as emails, blogs and social websites and applications such as Twitter and Facebook. In addition, direct contact with the participants can have an effect on their responses which can be minimised by using the questionnaire method.

On the other hand, there are some weaknesses in using a questionnaire in research. One drawback is that participants may not be encouraged to participate in the survey or complete it. In addition, respondents may not provide accurate, honest answers which can result in a validity issue. Another disadvantage is that it is difficult to follow up with the participants. In addition, no option to explain any difficult questions for the respondents (Fricker and Schonlau, 2002).

The sample size can be determined based on the size of the population which is studied in the research. In addition, the nature of the research and its objectives can affect the number of participants which is required in the study. Choosing the optimal sample size can lead to better results and findings.

4.5.2 Interviews

Interviews are considered as one of the most popular techniques of data collection in qualitative research (Ritchie et al., 2013). Interviews are usually managed in person whether through face-to-face conversation or via telephone or online video conference (Lee, 1991; Guba and Lincoln, 1994). The interviewer can use a formal or informal approach in managing an interview by discussing the subject generally with the

interviewee or asking the interviewee a number of listed predetermined questions about the topic (Denzin and Lincoln, 2011). Bless and Higson-Smith (2000) listed the following advantages for qualitative interviews:

- The interviewee can be involved actively in the process of the research.
- Interaction can be easily established between the interviewer and the interviewee.
- The interviewer can clarify any points which can help in catching the related data.
- The participants' ideas and thoughts can be collected in their own words.

In addition, it allows opportunities for selecting suitable participants for the interview which can help in saving more time and effort. In addition, the place and the time of the interview can be easily agreed between the interviewee and the interviewer.

The sample size used in interviews (qualitative research) is often smaller than the sample size of the quantitative research studies (Dworkin, 2012). The number of participants depends on the nature of the research and the ability to reach the required results. It is recommended that the required minimum size for interviews (qualitative studies) is at least 12 participants in order to collect accurate and reliable data (Braun and Clarke, 2006; Guest et al., 2006; Fugard and Potts, 2015).

4.5.3 Focus Groups

Focus group is considered one of the most common techniques used in qualitative research. Morgan (1996) defines a focus group as "a research technique that collects data through group interaction on a topic determined by the researcher". There are a number of merits which can be gained by employing focus group technique in the evaluation stage in this research. The most important advantage is that focus group can allow the researcher to ask questions attractively in order to encourage the participants to answer

the questions and talk freely about the subject being discussed (Krueger, 1997). This will enrich the discussion with valuable views, opinions and comments about the proposed framework.

In addition, the researcher can join the discussion to provide more explanations for the participants about any points in improving the discussion (Krueger and Casey, 2014). Moreover, the interaction between the group members during the discussion would improve the individual responses and shared opinions (Cohen et al., 2011). Furthermore, the researcher is able to take notes for the important points in the discussion and the whole session can be recorded.

The appropriate number of participants in each focus group depends on the purpose of the research and the type of participants. Most authors argued that that the appropriate number of participants in each focus group session would be between four and twelve people and the optimal number can be between 5 to 10 (Morgan, 1996; Sim, 1998; Beyea and Nicoll, 2000; Krueger and Casey, 2014).

4.6 Methods Adopted for Current Research

Having discussed research philosophies, paradigms research methods and data collection techniques used for conducting research in the previous section, this section discusses the methodologies and research techniques which can be used for this study.

As the main aim of this research is to develop a framework which can improve security management and awareness for home users which needs a repeated process of proposing, developing and evaluating artefacts. Therefore, the design science research, which was presented and discussed previously, was employed in this research. The work which has been done in this research is mapped to the design science research methodology defined

by Vaishnavi and Kuechler (2007) which has been already discussed in the previous section. Table 4.3 demonstrates the design science research processes which have been followed in this research. Problem awareness is the first stage in design science research. In chapter 2 and 3, the current information security awareness solutions, approaches and literature for home users were reviewed and investigated in order to identify the current gap.

The second stage of the design science process is the suggestions stage. A range of information security management frameworks, guidelines and best practices were reviewed in Chapter 5. In addition, a number of security controls and requirements were identified in Chapter 5 for different technologies and services which can be managed and monitored. These security requirements and controls were mapped to usable interfaces which have been designed based on HCI principles in Chapter 6. In addition, a participatory study (questionnaire) was conducted to get feedback from participants on the identified security requirements and the initial interfaces discussed and presented in Chapter 7.

<table>
<tr><th>The research objectives</th><th>Design science Stages</th><th>Process</th></tr>
<tr><td>1. To critically analyse the current information security awareness tools and approaches and identify the research gaps and opportunities.</td><td>Awareness of problem</td><td>Document analysis</td></tr>
<tr><td rowspan="3">2. To develop a novel approach to mapping complex security requirements in an adaptable manner; being mindful of technologies, services and people.

3. To design and develop flexible usable interfaces that inform and engage users, enabling improved awareness and management</td><td rowspan="3">Suggestions</td><td>Document analysis</td></tr>
<tr><td>Designing preliminary interfaces based on HCI principles</td></tr>
<tr><td>Participatory Study (Questionnaire)</td></tr>
</table>

4. To design a framework for improving information security management and awareness for home users.	**Development**	Design information security management and awareness framework
5. To conduct a series of evaluations involving stakeholders in order to measure the practical effectiveness and the usability of the proposed approach.	**Evaluation**	Evaluation of the framework (Focus group)
	Conclusion	Develop recommendations and limitations for the proposed framework

Adapted from (Vaishnavi and Kuechler, 2007)

Table 4.3: The Design Science Research Processes for This Research

The development stage is the third stage in the processes of design science research. The aim of this stage is to design and develop a novel framework for improving information security awareness and management (presented in Chapter 8).

The fourth phase is the evaluation stage which discussed the outcome of the framework evaluation. Two focus group sessions were conducted to evaluate the framework aspects, components and designs. This result of this stage was presented in Chapter 8.

The final and the fifth stage is the conclusion which discussed the limitations which can be identified and found from the results of the framework evaluation. In addition, the recommendations suggestions and future works of this phase were discussed in Chapter 9.

The current study used mixed methods, combining quantitative and qualitative methods (hybrid approach) guided by Design Science Research. The research starts with a quantitative approach applied through questionnaires in order to get more feedback to enhance the interface designs and final solution. As a final stage, a qualitative approach applied through focus groups in order to evaluate the final solution and framework.

Chapter 7 discusses the details of the questionnaire and Chapter 8 presents explanations on how the two focus groups which are conducted in this study.

4.7 Summary

The methodology chapter addressed the research methodology and approaches which were applied and used in order to achieve the aims of the research. This chapter primarily discussed different research paradigms and approaches used in the research field. In addition, it explained the research design, research approach, research methods and techniques used for the research. The design science research was selected for this research as it provides a framework that can help in achieving the required objectives. In addition, the questionnaire was selected as a method to assess the security concerns, knowledge and management for home users. It was also used to get feedback on the preliminary proposed interface designs. The focus group technique was used to evaluate the proposed framework and mock-up design. The next chapter discusses and reviews the current information security frameworks, standards and recommendations offered for large organisations, small business and home users in order to use the appropriate aspects and elements in the proposed approach.

Chapter Five

Information Security Management and Best Practices for Home Users

5 Information Security Management and Best Practices for Home Users

5.1 Introduction

End users are identified as the weakest element in the information security chain buy many studies and researches (Da Veiga and Eloff, 2010; Bashorun et al., 2013; Safa et al., 2016). Therefore, a number of security frameworks and standards including policies, procedures and guidelines are proposed for organisations and business sector in order to improve and manage information security effectively in order to provide satisfactory protection of the confidentiality, integrity and availability of data (Tipton and Nozaki, 2007). Implementing information security management approach including information security policy can be very effective to manage security and assets securely by mitigating potential risk and threats which might be caused by employees. In the work environment, all employees should improve their security behaviour and practices by obeying rules and guidelines in order to comply with the assigned security policies. However, home users do not have these organizational approaches which can help them in managing their security practices and controls effectively. They only use some security software such as antivirus and get advice and tips from public awareness websites such as Get Safe Online and Stay Safe Online.

The main for this chapter to discuss and review the current information security frameworks, standards and recommendations are offered for large organisations, small business and home users. In addition, it provides an overview of the information security policy and the current used in organisations. A further aim is to propose a number of security policies with different requirements and controls for different technologies, devices and services.

5.2 Information Security Frameworks and Tools

A wide range of security policy templates is available and accessible to be used in developing an information security policy document for organisations. These templates are not designed for a particular company but they can be improved and employed in creating security policy which can suit the organisation's vision and objectives. Different information security practices and well-known standards are used in organisations as a guideline to implement and manage security controls and configurations:

- ISO/IEC 27000 series: different ranges of information security standards are published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The most important two standards are ISO/IEC 27001 and 27002 and both are related to information security management. ISO/IEC 27001 provides an overview of the implementation requirements for information security management system. While 27002 mainly provides information and procedures on how to manage information security effectively in organizations. It offers security awareness topics, guidelines and controls which might be needed to protect information systems in organizations such as: operations security, human resources security, physical security and access control (International Organization for Standardization (ISO), 2013).
- NIST Special Publications: The US National Institute of Standards and Technology develops a wide of security publications including standards, guidelines, controls and policies to enhance information security in organizations. NIST published more than 500 documents related to information security and protection. Its 800 series provide extensive information and documents about

information security policies, procedures and guidelines which can be used to improve implementation and management of information security (NIST, 2019).

- CIS Critical Security Controls: The Center for Internet Security (CIS) published a set of defence actions and best practices known as CIS Critical Security Controls. The CIS Controls are used as a framework to help organizations to enhance information security within their networks and infrastructure. It prioritized set of actions which can be implemented to protect information assets in organisations into: basic, foundational and organisational. Recommendation and best practices are provided for several aspects such as email and web browser protection, data protection, malware defences and security configurations for router and firewall (CIS, 2019).

5.3 Recommendations and Best Practices for SME

Nowadays, all businesses use the internet, digital services and technologies in their daily activities. However, small businesses might not have enough resources including staff, technologies and budgets which can provide them with satisfactory protection of their information assets and services. As a result, several security approaches, frameworks, best practices and guidelines are offered for small and medium businesses in order to protect themselves from cyber security threats and mitigate any potential risk. This section reviews the academic literature for SMEs and the best practices and guidelines which have been provided by different specialised entities and organisation in the cyber security domain.

5.3.1 Literature Review on Cyber Security Management for SMEs

Osborn and Simpson (2015) argued that large organisations and small businesses do not use the same technology and security models and frameworks. The systems in SMEs are

not usually able to be improved and scaled because of the financial issues, system availability issues and insufficient security models and frameworks. Personal and cloud computing services could change the approach which has been applied to handle cyber security in SMEs. However, the existing cyber security practices in SMEs make users ill-served and ill-informed about the required security decisions (Osborn and Simpson, 2017).

Chapman and Smalov (2004) argued that SMEs usually do not succeed in implementing effective Internet and information security strategies due to lack of information security awareness, lack of technical skills and insufficient financial funds. They presented a sample mapping of the Computer Security Expert Assist Team (CSEAT) Information Security Review Areas onto the Alliance for Electronic Business (AEB) web security guideline. Five levels of effectiveness are provided for each answer to each security control question in order to measure progress toward effective implementation of security controls as presented in Table 5.1,

- Level 1 – control objectives documented in a security policy
- Level 2 – security controls documented as procedures
- Level 3 – procedures have been implemented
- Level 4 – procedures and security controls are tested and reviewed
- Level 5 – procedures and security controls are fully integrated into a comprehensive program.

AEB Topic	Level 1	Level 2	Level 3	Level 4	Level 5
Asset Classification and Control					
Listing of Assets					
What assets are owned by the web site, e.g. content and application data, web server?	Is there a policy that requires the listing of web site assets?	Are there procedures for listing web site assets?	Have web site assets been recorded?	Is there a periodic review to verify that web site assets are recorded?	Is recording of web site assets on a yearly basis standard business practice?
What assets are shared by the web site, e.g. network infrastructure?	Is there a policy that requires the listing of shared web site assets?	Are there procedures for listing shared web site assets?	Have shared web site assets been recorded?	Is there a periodic review to verify that shared web site assets are recorded?	Is recording of shared web site assets on a yearly basis standard business practice?
Are there any dependent assets, e.g. power supplies?	Is there a policy that requires the listing of dependent assets?	Are there procedures for listing dependent assets?	Have dependent assets been recorded?	Is there a periodic review to verify that dependent assets are recorded?	Is recording of dependent assets on a yearly basis standard business practice?
Are there any assets owned by third parties, e.g. information, services?	Is there a policy that requires the listing of third party assets?	Are there procedures for listing third party assets?	Have third party assets been recorded?	Is there a periodic review to verify that third party assets are recorded?	Is recording of third party assets on a yearly basis standard business practice?

Source: (Chapman and Smalov , 2004)

Table 5.1: Mapping CSEAT to AEB

Gupta and Hammond (2005) argued that the lack of security policies and procedures in small businesses make them more vulnerable to be victims for external and internal attacks and breaches. They suggested that the following best practices should be considered by small business owners:

- Participants in any transaction or tasks can be identified uniquely and clearly by establishing a process.
- Procedures are required to be implemented and available in order to control changes.
- Logs and activities need to be maintained and monitored by responsible staff.
- Features and backup services are important to be available systems and applications in order to avoid any business interruption or information loss.
- Data confidentiality between customers and vendors needs to be checked and ensured all the time.
- System architecture in small businesses should have the ability to avoid possible issues and repair themselves.

Keller et al (2005) tried to review and investigate the current threats and implemented controls and best practices in small businesses by conducting one-to-one interviews with 18 small companies. They found that 59% of the companies have experienced internal attacks which can be caused by human errors or misuse. Around 28% have had Trojan attacks while 22% have been attacked by hacker or viruses. In addition, they recommended the following best practices for small businesses based on their findings from the 18 companies:

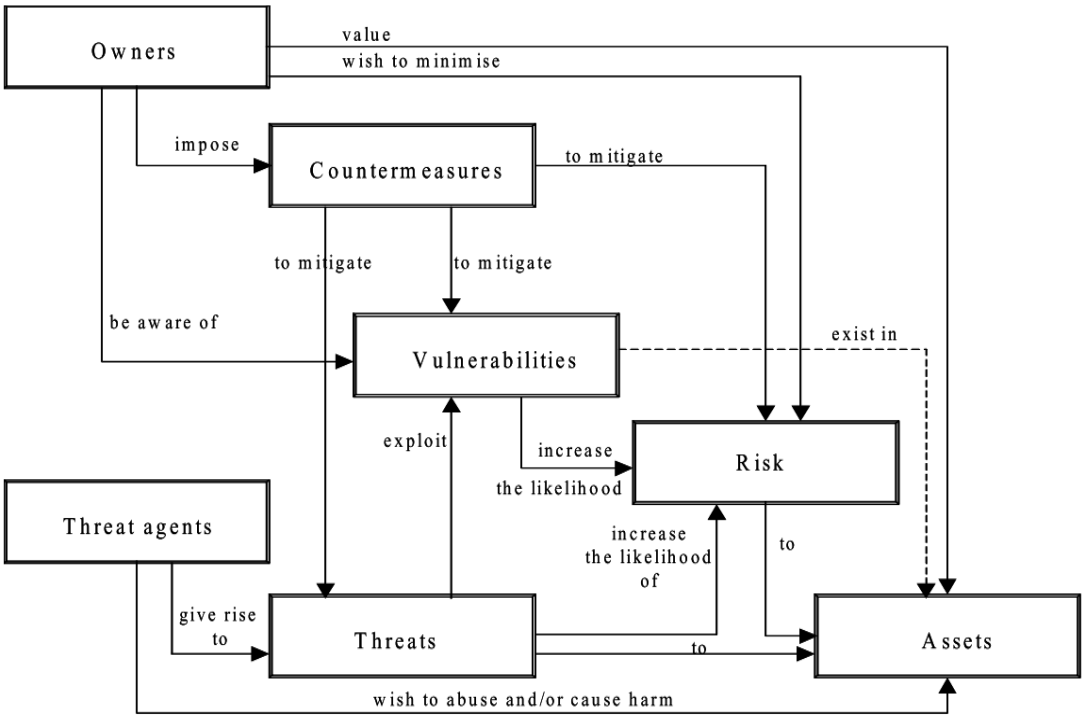
- Install and properly configure firewall
- Update software.

- Protect against viruses, worms and Trojans.
- Implement a strong password policy.
- Implement physical security measures to protect computer assets.
- Implement company policy and training.
- Connect remote users securely.
- Lock down servers.
- Implement identity services (intrusion detection).

Morgan (2006) investigated the security problems potential impacts of security breaches which van be experienced by small business. Several suggestions for procedures and solutions are offered in order to improve cyber security and mitigate potential threats in small business environment. The first procedure is to create and implement security policies for different aspects such as acceptable use, physical security and internet access. Another recommendation is to apply physical security for the technological and information assets by locking down servers and other equipment. In addition, implementing and managing firewall, antivirus and intrusion detection system is important to provide better cyber security management. Furthermore, the wireless LAN needs to be managed and configured securely. Also, regular backup for the system and information is an important task in information security implementation. Another recommendation is to educate all users about appropriate access methods and how to deal with data and technologies safely.

Onwubiko and Lenaghan (2007) proposed a conceptual framework which aims to assist SMEs to mitigate and prevent effectively cyber security threats and potential vulnerabilities. The proposed framework is adapted from ISO/IEC 15408 by defining seven security concepts and the relationships between them as presented in Figure 5.1.

The conceptual framework can help organisations to identify and understand what is the areas need to be protected (assets), what kind of threats should be protected from (vulnerabilities, threats and risks) and how these assets can be secured and protected (countermeasures). Firstly, the essential assets for SME are identified and recognised by the framework by determining what kind of assets need to be protected and existing weaknesses in these assets. Secondly, the associated and potential threats which can be exploited by the existing weakness and vulnerabilities are identified and covered. Finally, a list of recommendations and countermeasures are provided which can help in preventing and mitigating the identified vulnerabilities and potential threats.



Source: (Onwubiko and Lenaghan, 2007)

Figure 5.1: Security Conceptual Framework for SMEs

Sangani and Vijayakumar (2012) stated that SMEs do not have their own security measures policy which is applied in large organizations. They tried to propose an Information Security Assurance Cyber Control for SMEs (ISACC) against common cyber

security threats implemented at a cost effective. The following common cyber security threats for SMEs have been identified, reviewed and recommendations and best practices have been suggested to mitigate these threats:

- Phishing.
- Web Application Attacks.
- Insider Attacks.
- Wireless network breaches.
- Wi-Fi Hotspots.

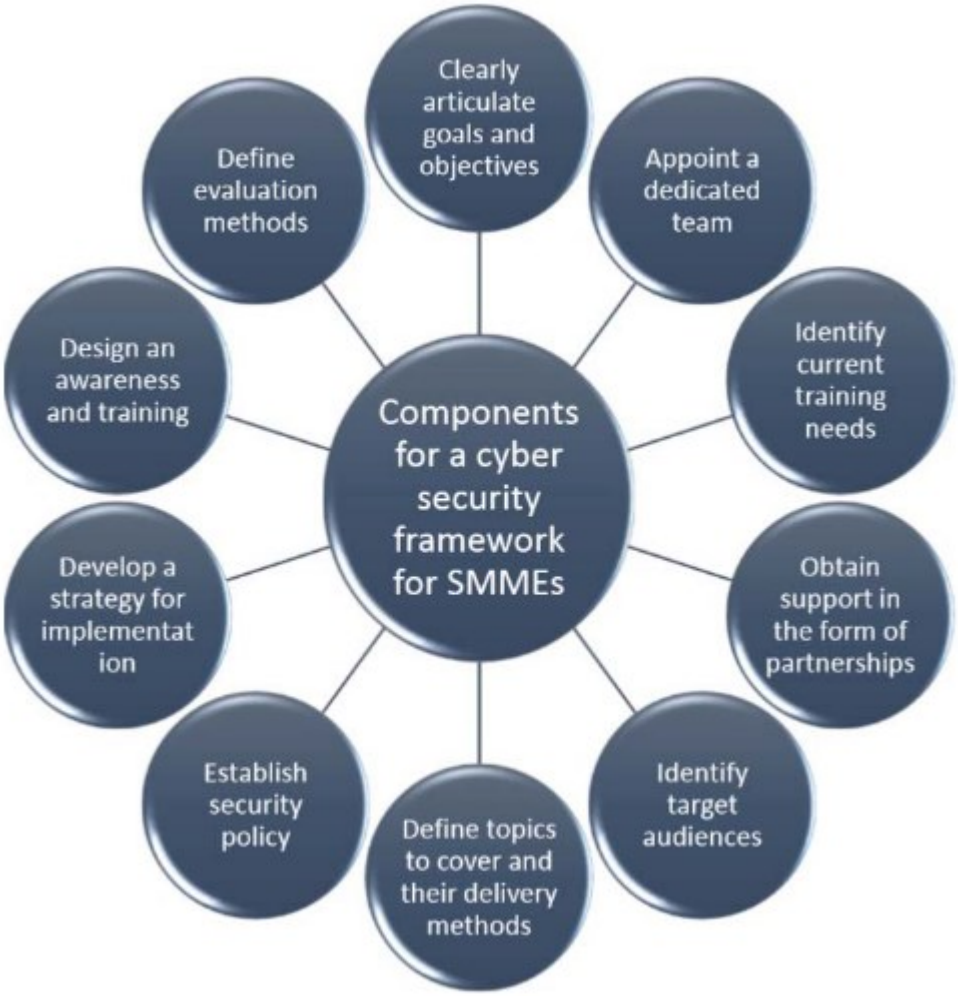
Von Solms (2015) stated that small businesses and companies are increasingly becoming major targets for cyber security attacks and threats in South Africa. Therefore, a plan of action is proposed to improve cyber security for small companies in South Africa. The proposed plan includes 5 categories:

- Providing a Cyber Security Public-Private Partnership (CSPPP)
- Providing a web portal for Small Company Cyber Security.
- Providing Cyber Security Awareness (CSA).
- Providing Cyber Security Technical initiatives (CST).
- Providing better Cyber Security Capacity Building (CSCB)

Berry and Berry (2018) tried to assess the approaches which have been implemented by small businesses for mitigating cyber security threats and improving risk management. They interviewed 373 respondents from different types of small businesses. They found that mod the small businesses have implemented some physical access policies and technical solutions such as anti-virus and firewall. However, the result showed that the respondents, who are responsible for managing these technologies, did not maintain and

update these security solutions properly. In addition, most of the respondents did use strong passwords or change them regularly. They suggested that policies procedures and practices in small businesses need to be changed and improved in order to mitigate possible cyber security threats.

Lejaka et al. (2019) argued that small, medium and micro enterprises (SMMEs) in South Africa do not always pay attention to cyber security issues. Therefore, they proposed a cyber security awareness framework which can be used by SMMEs. The proposed framework has several components as presented in Figure 5.2.



Source: (Lejaka et al., 2019)

Figure 5.2: Components of A Cyber Security Awareness Framework for SMMEs

5.3.2 Cyber Security Guidelines and Best Practices for SMEs

Woody and Clinton (2004) argued that some of the common information security standards and frameworks might not be effective for small businesses. Therefore, they suggested a list of best practices which can be considered for SMEs:

- Use strong passwords with regular change.
- Be cautious with email attachments and internet downloads.
- Install antivirus software and update it.
- Install and use a firewall.
- Remove unused software and user accounts.
- Create regular backups for important files.
- Keep systems and software updated.
- Implement good network security with access control.
- Limit Access to sensitive data.

The UK National Cyber Security Centre (NCSC, 2018a) proposed another cyber security guidance for small organizations:

- Implement secure configuration such as passwords, patching and disabling unnecessary settings.
- Implement security procedures for home and mobile working.
- Establish incident management policies and procedures.
- Install malware and virus prevention software.
- Manage and review user privileges to remove unnecessary access rights
- Monitor systems and services to avoid any potential risk or attacks
- Create a secure network by implementing security policies and technical responses.

- Apply appropriate security controls and procedures for using removable media such as USB and CDs
- Support end-users with education and awareness programs.

Another similar guideline was offered by Aleksandrova (2015). It includes several tips and advice such as secure configuration, firewall, access control and administrative privilege management, patch management and malware protection. National Institute of Standards and Technology (NIST) offered a cyber security guideline for small business (Toth and Paulsen, 2016):

- Identify and control who has access to your business information
- Conduct Background Checks
- Create policies and procedures for information security
- Manage and limit access to data and information
- Patch systems and applications.
- Install and activate firewall.
- Install and update antivirus, spyware, and other malware programs.
- Configure a secure wireless access point
- Set up web security
- Use encryption for sensitive information
- Disposal procedures for old computers and devices safely.
- Educate and train end-users on how to behave safely.
- Make regular and full backups of important data.

Department for BIS (2015) suggested several security tips which might be necessary for small business such as malware protection, firewall , secure wireless network, secure system configurations, regular management of user privileges and removable media

control. Information Commissioner's Office (2016) produced another cyber security guideline for SMBs. It includes several measures which need to be implemented in order to get protected: assessing the threats and risks, configure firewalls, secure configuration, access control, malware protection, patch management and software updates, Encryption and data backup. IBA (2018) proposed a cybersecurity guideline for small business, including the following measures and tips to enhance information security:

- Implement strong username and password management
- Keep system software updated
- Implement endpoint protection
- Use secure internet connections
- Secure web browsing and email.
- Implement data retention, loss recovery capability
- Encrypt data and devices
- Enable remote erasure
- Strictly manage access control.
- Consider application whitelisting/blacklisting.
- Secure mobile devices.

5.4 Recommendations and Best Practices for Home Security

A recommendation guideline was provided by SANS Institute for building a secure home network (Thomas, 2001). This guideline includes virus protection, firewall configuration, wireless access point security, password security, backup and Internet browser security.

The ITU Telecommunication Standardization Sector introduces ITU-T Recommendation X.1111 which describes security threats and security requirements which should be considered to protect home network and home users (ITU, 2007). The standard illustrates

the following security requirements which need to be considered in home network: data confidentiality, data integrity, authentication, authorization, non-repudiation, communication flow security, privacy security and availability. In addition, it presents the following security functions for satisfying security requirements in the home network: encipherment function (or encryption), digital signature function, access control function, data integrity function, authentication function, notarization, message authentication code (MAC) and Key management function.

Another range of recommendations and tips is provided by US-CERT for improving home network security by offering home users information about security risks and countermeasures (US-CERT, 2001). These include firewall, antivirus, email security, backup, internet browser and operating system security. Another security advice and guideline called "Security Tip (ST15-002)" is offered by US-CERT (2015). It includes recommendations for improving password security, wireless security, email security, antivirus, firewall and backup.

In addition, NSA (2016) provides best practices for keeping home network secure and helping home users to implement security controls and configurations. The guideline offers security tips and recommendations, including: operating system updates, security suite such as antivirus and firewall, strong and protected passwords, limit administrator accounts, install and update software from trusted sources, implement WPA2 on wireless.

Department of Digital, Culture, Media & Sport (DDCMS, 2018) proposed a code of practice for consumer IoT security. It includes a wide range of recommendations such as: no default passwords, implementing a vulnerability disclosure policy, keeping software updated, securely store credentials and security-sensitive data, communicate securely, ensure that personal data is protected.

Corser et al. (2017) offered best practices for the internet of things (IoT). It includes several tips and advice such as: making hardware tamper resistant, providing for firmware updates/patches, performing dynamic testing, specifying procedures to protect data on device disposal, using strong authentication, using strong encryption and secure protocols.

Get Safe Online (2011) delivered another security guideline which contains a number of cyber security tips such as installing security software (firewall, antivirus), keeping system and applications updated, implementing strong passwords, using encryption, implementing email security, wireless security, configuring and check the security and privacy settings on web browsers. Performing a regular backup, Limiting access, downloading software and applications from trusted sources, implementing portable hard drives security and control and educating other users on how to get protected online.

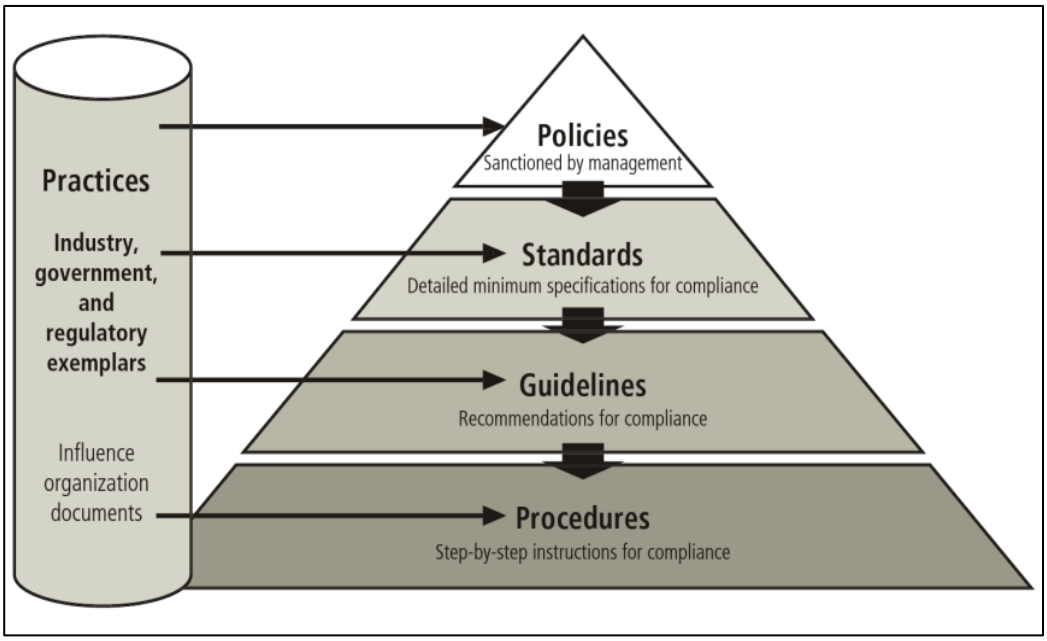
All the above frameworks, best practices and guidelines are proposed and offered in order to help organizations and home users in keeping their information, devices, systems and services protected and secure. Using information security policy has been recommended by a number of security frameworks for organisations in order to manage and monitor their security effectively. The next section discusses the importance of information security policy and its types.

5.5 An Overview of Information Security Policy

Information Security policy is a formal document which contains rules and guidelines which need to be followed by end-users in order to manage information assets and technologies securely (Peltier, 2016). NIST (2014) defined a security policy as "an aggregate of directives, rules, and practices that prescribes how an organization manages, protects and distributes information". Having well-defined security policies and

procedures in organizations is as vital as the other security technologies such firewall and antivirus software (Knapp et al., 2009). Therefore, information assets and services cannot be secured by only implementing different technical solutions without having policies and procedures.

Kamariza (2017) argues that policies should be created by senior management with high-level statements connected to information security in the organisation. In addition, security roles, responsibilities and scope of the information should be described in the policy. Standard, procedures, guidelines and practices should include this type of information. Whitman and Mattord (2016) explain the relationship between policies, standards, guidelines, procedures and practices as shown in Figure 5.3. For example, username and a strong password are required to access a network server can be set as policy. The standard can include the length or the complexity of the password while the guidelines might advise not to use the family name as password. Practices can provide some tips such as changing password at least twice a year.

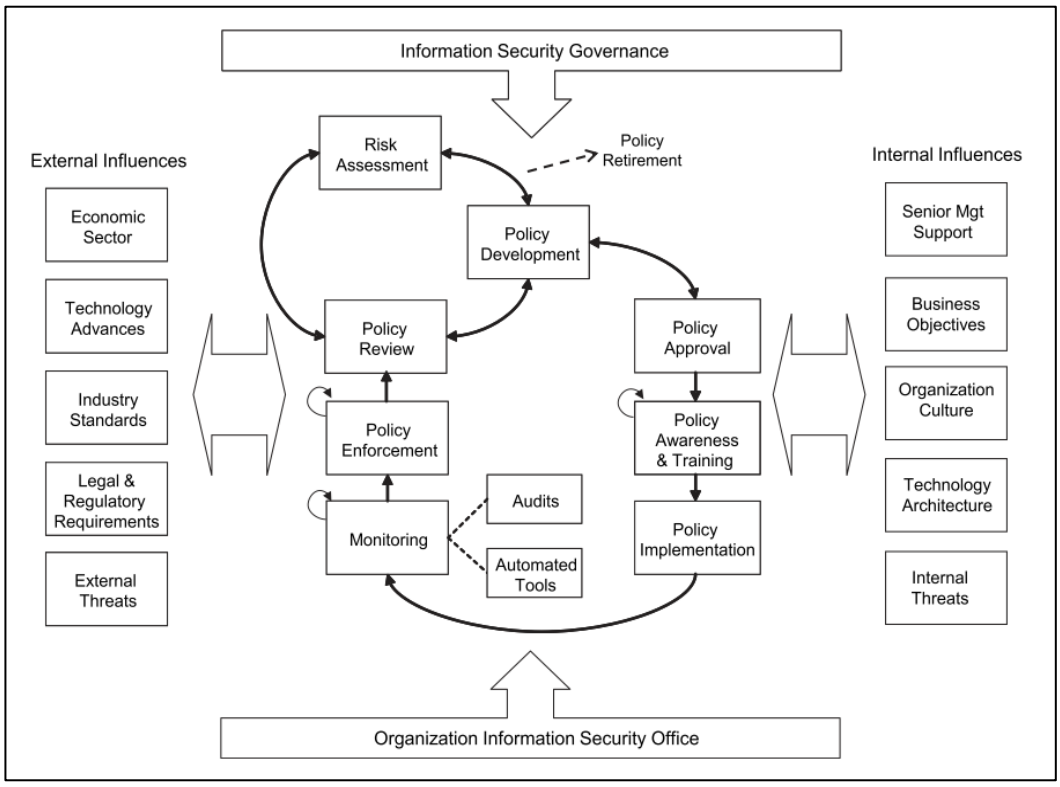


Source: (Whitman, 2014)

Figure 5.3: Policies, Standards, Practices, Procedures and Guidelines

The need for security policies, processes and procedures becomes more important when there is a need to mitigate internal threats or minimize the possibility of security incidents or threats that can affect information assets and services in organizations (Knapp et al., 2009). Therefore, having security policies with rules, guidelines and measures which can be applicable for home environments can help in managing different security controls and configurations properly which can enhance and improve security practices for home users(Howe et al., 2012; Rao and Pati, 2012; Nthala et al., 2018).

Knapp et al. (2009) illustrate the process of information security policy in organizations as shown in Figure 5.4. In this mode, external and internal influences can affect the process of information security policy. It can be seen that the process of managing information security policy includes: risk assessment, development, approval, awareness and training, implementation, monitoring, enforcement and policy review.



Source: (Knapp et al., 2009)

Figure 5.4: Comprehensive Information Security Policy Process Model

A continues risk assessment and policy development and review is very important in the process of information security policy in order to mitigate new threats or possible risk which are not covered or managed by the security policy in order to provide good protection for information assets, services and technologies.

5.6 Types of Information Security Policies

Information systems and technologies have been used widely in organizations and become an essential element in their daily business procedures. Therefore, it is important to protect their information assets, networks and services by implementing different types of controls and security measures. A wide range of security policies have been implemented and used in organizations, some examples are listed in Table 5.2:

Clean Desk Policy	Information Protection Policy
Access Control Policy	Special Access Policy
Remote Access Policy	Email Security Policy
Firewall Management Policy	Acceptable Use Policy
Remote Access Policy	Mobile Device Policy
Password Policy	Network Security policy
Physical Security Policy	Encryption Policy
Data Breach Response Policy	Wireless Communication Policy

Table 5.2: Information Security Policy Types

The SANS Institute published free information security policy templates which can be used by business to promote information security process and procedures. Different security aspects and topics are included in the templates such as password construction, password protection, email use and wireless communications SANS (2014). These templates need to be changed and updated based on the security requirements and infrastructure for each organization in order to be suitable and effective. The following section illustrates some of SANS policy templates which provide practical measures and controls for end-users.

5.6.1 Password Protection Policy

Password is considered one of the most common authentication methods which can keep data and services protected and confidential. Several best practices, guidelines and procedures are proposed to help in choosing and managing passwords in order to help end-users and organizations to mitigate any potential risks or threats. The aim of password protection policy is to offer a set of rules and standards in order to enhance password security by creating strong secure passwords and managing them securely. For example, SANS (2014) designed a password protection policy template which has the following elements:

1. **Password Creation**
    - All users must conform to the password construction guidelines suggest by SANS:
        - The length of the password should be satisfactory (14 characters recommended)
        - It is recommended to create passwords with multiple words.
        - Avoid using passwords with personal information such as birthdates and phone numbers.
        - Avoid using a common weak password such as “Password123” and “aaabbb”
    - Users must use a separate password for each service account in the organization.
    - Users may not use any passwords related to the organization’s accounts for their own, personal accounts.

- Some form of multi-factor authentication can be used for any privileged accounts.

2. **Password Change**
   - Passwords should be changed regularly such as every 3 or 4 months or when there is a need to change it such as being compromised.
   - Password cracking or guessing tools can be used by IT security team to check the strength of the used passwords.
3. **Password Protection**
   - Passwords must not be shared with anyone
   - Passwords must not be written in emails or revealed over the phone to anyone.
   - Do not save passwords and login information in web browsers
   - Any security incidents or doubt that the password has been compromised must be reported.

5.6.2 Wireless Communication Policy

Wireless access points with weak security settings can lead to authorized access and attacks that can expose critical assets and confidential information. Employees can have the ability to access their corporate network by using their home wireless devices. Therefore, it is very important for organisations to make sure that all wireless success points used to access their networks are configured and managed with the best practices and policies agreed by organizations. SANS suggested some criteria and settings which need to be applied in home wireless in order to protect employee and corporate data. All home wireless devices must adhere to the following:

- Enable WiFi Protected Access Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLSWhen enabling WPA-PSK.
- Configure a strong shared secret key (at least 20 characters)
- Disable broadcast of SSID
- Change the default SSID name
- Change the default login and password

5.7 Initial System Requirements for Improving Security Management and Awareness for Home Users

It is envisaged that a novel architecture will have the core functionality which can allow the proposed system to identify, check and manage the security configuration and practice in devices connected to the home network. In addition, the proposed security management system can enhance awareness amongst home users by providing them with bespoke awareness when it is needed. Several requirements need to be considered in order to offer an effective security management system:

- The system should have the ability to offer tailored security awareness should be based on the users' current needs. As it was identified in the literature review that there is a lack of providing users with bespoke awareness. Providing bespoke awareness can be a good opportunity for enhancing users' knowledge and encourage them to learn more in a usable manner. This can be delivered by implementing security policies which can monitor and manage different security controls and make users aware of any potential threats or issues.
- Different groups of security policies can be defined and assigned for different devices and users. The policies can manage and monitor different operating systems and technologies including their security configuration, settings and

controls which can enhance their protection and security as suggested in the by a number of studies in the literature review.

- Pre-defined security policy templates can be provided for home users in order to manage different security controls in different devices with different users. These templates will have different security requirements based on the technology or the operating system. For example, a pre-defined template can be called password policy which can include most of the password settings and requirements which can be implemented in desktop and laptop devices. Section 5.7.2 provides more detail about the pre-defined templates.
- Different security levels can be provided for the security policies such as low, medium and high. This will provide good flexibility in the functionality of the system in order to meet the users' needs.
- The components and the interfaces of the system should be usable easy to access, use and understand in order to help the system to achieve its main objectives and goals. Therefore, the next chapter (chapter 6) will propose a number of preliminary interfaces which are designed based on HCI principles.

The following subsections discuss some of these requirements which are suggested to be considered in the proposed framework for improving information security management and awareness for home users.

5.7.1 Information Security Policies for Home Networks

From the above security frameworks, guidelines and best practices, several security practices can be suggested in order to enhance cyber security for home users, home networks and digital devices. Table 5.3 shows a number of identified security areas with relevant best practices including but not limited to password security, software security,

endpoint protection, data protection and web browsing security, internet connection security and removable media security.

Security Area	Recommended practices
Password Security	Implement strong username and password management
Software Security	Keep system software and applications updated
Internet Connection Security	Use secure internet connections
Endpoint Protection	Install antivirus software
Endpoint Protection	Configure firewall protection
Web browsing Security	Configure web browsers securely
Data Protection	Encrypt data and devices
Data Protection	Enable remote erasure
Software Security	Consider application whitelisting/blacklisting
Software Security	use apps from a trusted source
Data Protection	Back up data
Removable Media Security	Manage and limit the use of removable media such as USB sticks, memory cards, CDs and DVDs.

Table 5.3: The Security Best Practices Recommended for Home Network and Devices

There are several devices including, but not limited to, Computers, laptops, smartphones, tablets, smart TVs and wireless access points which are selected and categorized into four different groups as they are the most popular digital devices used by home users as evident by Ofcom (2019):

- Desktop PCs and Laptops group.
- Smart Phones and Tablets group.

- Smart TVs and Game Consoles group.
- Wireless access points

The above information security management frameworks for organizations and best practices for SMBs and home networks are used to identify some the processes and controls which might be applicable to be implemented for the home users in order to create and design several information security policies which includes a number of security features and controls which need to be configured, managed and monitored securely. In addition, the official user guide documents for the devices with different operating systems have been reviewed in order to identify the most common security settings and configuration based on the best practice of security in each device, technology and service. Table 5.4 shows the popular common operating systems which have been selected and reviewed in order to identify the most common security controls and configurations.

Computers & Laptops	Smartphones & tablets	Smart TV	Game Console
Windows Mac	IOS Android Windows	Google TV Android TV Firefox OS	PlayStation system Xbox system

Table 5.4: The Reviewed Operating Systems and Technologies

The following Security policies can be proposed to monitor and manage the security configurations for different technologies at homes by applying them in the proposed tool:

- **Password policy:** it contains the password settings which can be implemented in the devices such as minimum password length and password complexity.

- **Device security policy:** it contains the security features and controls which should be implemented and configured in the devices such as firewall and anti-virus software.
- **Software policy:** it includes all the security configurations required to be managed in order to provide security for the applications and software such as disabling the new installation and preventing the download from unknown sources.
- **Internet browser policy:** it contains the security settings and configurations which should be managed and monitored in each internet browser such as Pop-Ups blocker and saving login information.
- **Backup policy:** it has the configurations which are related to the backup and restoring process in the devices such as enabling the backup option and scheduling the backup.
- **Parental controls policy:** it contains the configurations which can be implemented and applied for managing the parental controls in the devices.

Table 5.5 presents a number of different groups of security policies which can be applied and measured in computers including desktop PCs and Laptops.

Category	Policy Statement	
Password Policy	• Enable password • Configure maximum Password Age • Enable password Complexity • Configure account lockout threshold for Invalid logins	• Configure minimum Password Length • Configure Enforce Password History • Configure Account lockout duration • Enable Time before auto-lock

Software Policy	• Enable administrator account for new installation • Block new Installations	• Disable specified applications • Configure whitelist applications • Configure blacklist applications
Device Security Policy	• Enable firewall • Download latest OS version • Virus Protection • Enable Anti-virus software update • Enable OS Auto update	• Control CD/DVD-ROM Drive • Control USB port • Enable locate the device • Enable remote wipe • Enable Notification
Internet Browser Policy	• Disable saving sign-in info (username, password) • Disable auto-fill information • Enable web browser auto update • Enable unsafe website warnings • Disable plugins downloaded from untrusted sources • Enable Pop-Ups blocker • Disable collecting or tracking browsing data.	• Block third party cookies and site data • Delete the browsing history when closing the browser • Security level of Internet zone for internet Explorer • Enable where to save each file before downloading • Enable clearing cookies and site data when you quit browser • Disable location tracking
Backup Policy	• Enable backup setup option • Configure backup contents	• Configure backup Schedule time
Parental Controls Policy	• Enable parental control • Configure game rating	• Configure time limits • Configure programs limits

Table 5.5: The Identified Security Policies for Desktop Pcs and Laptops

Table 5.6 shows several security policies which contain different security configurations and settings which can be configured and implemented in most of the smartphones and tablets. The password policy has been added to the device security policy in the smartphones and tablets group because most of the password policy statements above are not applicable to the smartphone and tablets.

Category	Policy Statement	
Device Security Policy	• Enable Security lock • Enable time before auto-lock • Enable fingerprint • Enable auto wipe after 10/15 failed attempts • Download latest OS version • Enable OS Auto update • Enable firewall • Install virus Protection	• Enable anti-virus software update • Enable notification • Configure SIM card PIN • Device compromised? "Rooting" or "Jailbreaking" • Enable locate the device • Enable remote wipe • Control CD/DVD-ROM drive • Control USB port
Software Policy	• Enable authentication for purchases • Enable Auto update download for apps • Enable parental control in the application store	• Manage third-party apps request access to personal information such as contacts, calendars, photos and camera, location • Disable installing apps from unknown sources.
Internet Browser Policy	• Enable Pop-Up blocker • Enable unsafe website warnings • Enable auto fill option • Disable collecting or tracking browsing data. • Disable saving sign-in info (username, password)	• Block third party cookies and site data • Ask where to save each file before downloading • Disable plugins downloaded from untrusted sources • Disable location tracking
Backup Policy	• Enable backup option • Configure backup contents	• Configure backup Schedule time
Parental Controls Policy	• Enable parental controls • Configure game rating	• Configure time limits • Configure programs Limits

Table 5.6: The Identified Security Policies for Smartphones and Tablets

The smart TVs and game consoles have less security settings, configurations and controls than the computers and smartphones. As a result, most of the security settings and configurations which can be applied in smart TVs and game consoles are added in on policy called device security policy as presented in Table 5.7.

Category	Policy Statement
Device Security Policy	• Enable parental control • Enable passcode • Enable Pop-Up notifications • Enable automatic update • Disable saving sign-in info (username, password) • Disable auto fill option • Disable installing apps from unknown sources • Download latest OS version

Table 5.7: The Identified Security Policy for Smart TVs and Game Consoles

Table 5.8 shows most of the important security configurations which need to be managed, checked and controlled in the wireless broadband devices.

Category	Policy Statement
Device Security Policy	• Enable WiFi Protected Access Pre shared Key • Download latest OS version • Disable wireless SSID broadcast • Enable MAC address filtering • Configure Strong shared secret key

Table 5.8: The Identified Security Policy for Wireless Access Points

5.7.2 Pre-defined Policy Templates

It is very beneficial to create and design a number of pre-defined security policy templates for different security aspects and areas in order to provide better cyber security. These pre-defined templates can be pre-designed and pre-configured by the administrator or expert staff in the domain in order to produce the best results. This can ensure that all the rules and policies are defined and configured effectively. In addition, the templates can provide more consistency and clarity for both administrators and end-users which can provide better security management. Administrators can easily change the configurations assigned in templates based on the current needs or the used security standards.

For example, windows provide a local security policy console which can be used for configuring a security policy setting on the local device, a domain-joined device, and on a domain controller. Different settings can be configured and managed via the policy editor. In addition, a new policy template can be imported in a local device as shown in Figure 5.5.

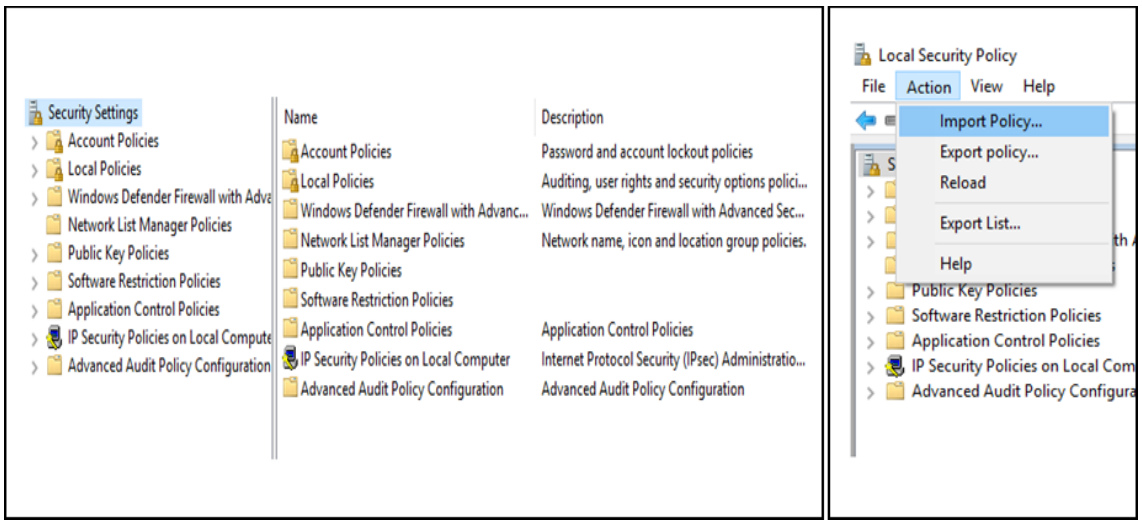


Figure 5.5: A Screenshot of The Local Security Policy in Windows

A password policy template is provided which includes the most important settings and configurations which can be implemented for password policy such as minimum password length and enforce password history as shown in Figure 5.6.

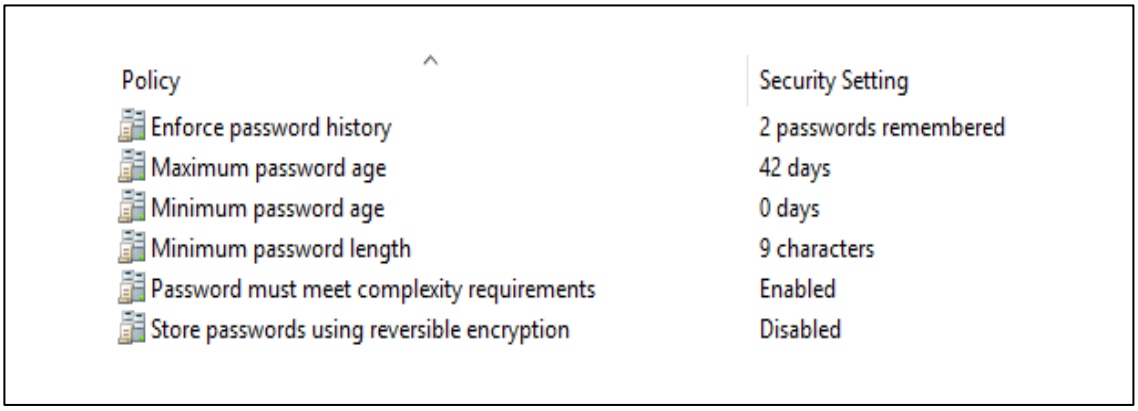


Figure 5.6: A Screenshot of Password Policy in Windows

The assigned value for each setting can be changed in order to meet the required security criteria or comply with the information security standard used in the organisation. In addition, an explanation is offered to give more information about each policy statement as shown in Figure 5.7.

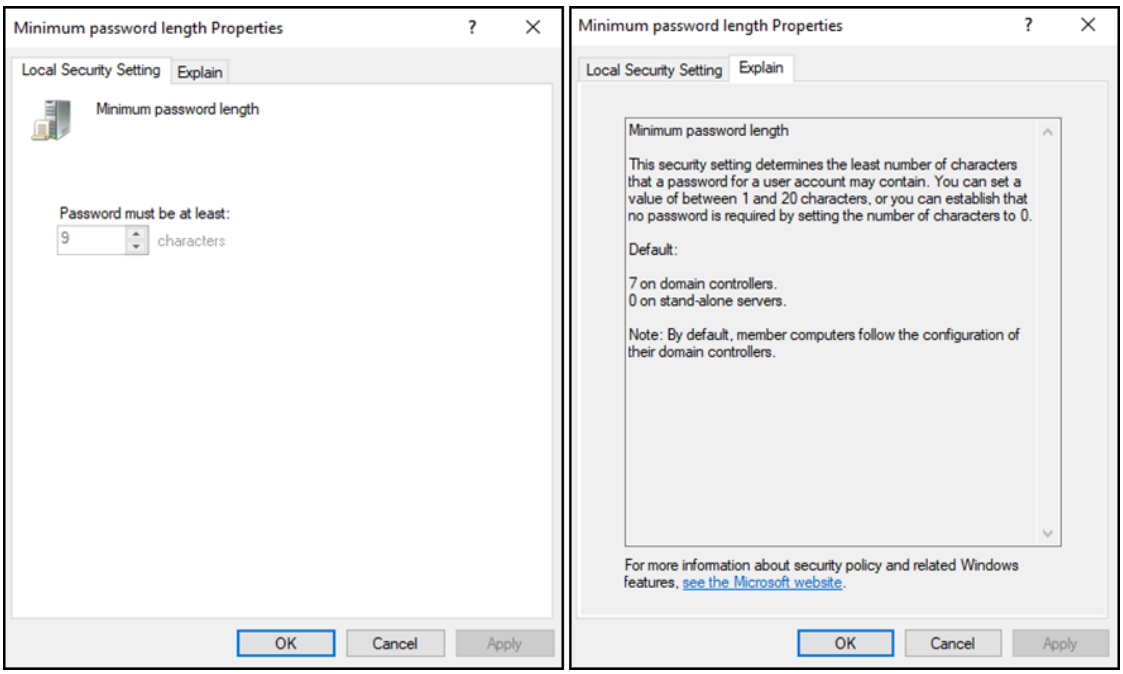


Figure 5.7: A Screenshot of Minimum Password Length Properties

5.7.3 Security Policy Levels

Novice users do not have enough knowledge to configure all the security settings and controls with the best-recommended practices. This lack might prevent novice users from applying the appropriate required settings. Therefore, different security levels can be provided for each policy statement in order to provide more granularity and flexibility which can help in satisfying the user's needs and requirements. It can be suggested that the security policies can be configured and defined based on three levels: low, medium and high:

- Low level: it can contain the minimum requirements (baseline) which need to be configured in the devices and it can be assigned for novice users who do not have good technology experience.
- Medium level: it can contain most of the security controls and requirements with security settings better than the ones at low level.
- High Level: it includes all the security configurations and controls which need to be configured and managed with strong security rules and standards.

Table 5.9 illustrates an example of how the three security levels can be configured and defined for password policy statements. These settings are suggested and can be changed based on the applied standard for each security level. This can help in mapping complex security requirements in an adaptable manner which can promote security management and awareness for home users. The guideline provided by NCSC (2018b) for improving password administration and security in technologies is used to propose the required configurations and option which need to be configured and defined for the bassline level (low level). The NCSC guideline suggested the following points which can be considered for the password administration:

- A minimum password length should be specified to prevent very short passwords from being used.
- The capabilities of systems and technologies should be considered when defining password length.
- Excessive long passwords should be avoided in order to make it easy for users.
- Complexity requirements should be disabled when creating passwords in order to avoid any extra burden on users.

- Regular password expiry should be avoided because it might harm rather than improves security.
- Users should be given between 5 and 10 login attempts before locking out accounts.
- Automatic locking out should be configured for inactive accounts.

All the above recommendations have been considered and suggested as baseline level (low level) which can provide the minimum level of password security requirements as presented in Table 5.9.

	Policy Statement	**Indicative Parameter for The Security Level**		
		High	**Medium**	**Low**
Password Policy	Minimum Password Length	10 characters	10 characters	8 characters
	Password Complexity	Enabled	Enabled	Disabled
	Enforce Password History	3 passwords	2 passwords	1 password
	Account lockout duration	5 minutes	5 minutes	Disabled
	Account lockout threshold for Invalid logins	5 Invalid login attempts	5 Invalid login attempts	10 Invalid login attempts
	Time before auto-lock	3 minutes	5 minutes	10 minutes

Table 5.9: Suggested Password Policy with Three Levels

5.8 Summary

Most of all the large organizations have already implemented information security frameworks and standards to manage and monitor their security assets. Several best practice guidelines and recommendations are proposed to improve information security management and practices for small and medium enterprises, as they do not have enough

budget to invest in their cyber security and technologies. Most of information security standards and guidelines emphasize that information security policy is an essential element in information security management. A wide range of security policies can be established to control and manage different services, technologies and security aspects such as password, email and web browsing security policy. A variety of recommendations and best practices offered for keeping home networks and digital devices secured and protected. However, implementing these recommended requirements mainly rely on the willingness, desire, skills and knowledge of individual users as there is no centralized system which can manage and monitor different controls and configuration in different devices. Therefore, a number of security policies with different security requirements and security aspects for different technologies and services are proposed and created, after discussing and reviewing information security standards, guidelines and best practices for large organisations and SMEs alongside with the recommendations and guidance for home cyber security.

The concept of using security policies will be validated by asking specific questions in the participatory study in order to investigate the effectiveness of using security policies. It will be also followed by conducting a focus group session and discussing with experts whether using security policies is an appropriate way for improving information security management and awareness.

The following chapter will illustrate how the identified initial security requirements and policies can be applied and visualized to monitor and manage security practices and controls different users and devices in a usable effective manner in order to promote information security management and awareness for home users.

Chapter Six

HCI Principles and

Preliminary Interfaces

6 HCI Principles and Preliminary Interfaces

6.1 Introduction

With the development of information technology and computer software, the need and the importance of understanding how humans use and interact with computing devices have increased. Designing an interactive system for human use is considered one of the key concerns can be experienced in the field of human-computer interaction (HCI) (Dix, 1998; Huang, 2009). Thus, Several HCI guidelines and principles have been introduced to enhance the development of user interface elements including usability, efficiency and consistency. Dix (1998) stated that understanding that people want to use systems easily without any difficulties have to be considered in the process of designing digital devices and applications. The main aim of HCI is to make the interaction between users and computers very easy and effective. Hewett et al. (1992) defined human-computer interaction as "a discipline concerned the design, evaluation and implementation of interactive computing systems for human use and with the study of major phenomena surrounding them".

The main for this chapter to provide some definitions of HCI. In addition, it discusses the importance of HCI concepts and principles and reviews the current information security frameworks, standards and recommendations are offered for large organisations, small business and home users. In addition, it provides an overview of the information security policy and the current used in organisations. A further aim is to review general usability guidelines for designing interfaces and usability guidelines for security applications. In addition, A number of preliminary interfaces are proposed, designed and presented which can visualise for the main components and elements of the proposed framework for improving information security management and awareness for home users.

6.2 The Importance of Human-Computer Interaction (HCI)

Human-computer interaction (HCI) focuses on the interaction between users and computers by using the components in the user interface. A number of HCI concepts have been established to enhance the process of the interface design whether a new interface or improving an existing interface in terms of usability and effectiveness in order to meet the need and satisfaction of the main stakeholders: end-users (Muñoz-Arteaga et al., 2009). The importance of HCI has been highlighted in a variety range of studies which emphasize that HCI can help in ensuring the functionality, usability, effectiveness of systems and improve user experience (Fetaji et al., 2007; Kendall and Kendall, 2010; Feizi and Wong, 2013). Scholtz et al. (1999) stated that the need for HCI is important to deliver the advantages of information technologies and communications and being used by users and organisations effectively. Generally, HCI helps in making systems and applications more usable, useful and receptive to user's needs.

On the other hand, there are some key issues and challenges which can make HCI less effective. One of the Technical design issues which can be experienced is the limited screen size for mobile devices which can make the presentation of information and navigation difficult for users. In addition, hardware issues such as limited input and output facilities and designing for mobility can be faced while developing systems. Aside from the hardware issues, other challenges related to software can be experienced in HCI design for mobile devices such as Hierarchical menus, navigation, browsing, images, icons (Huang, 2009). Myers (1994) stated that some interfaces and components are difficult to be designed and implemented by specialists which make HCI failed in achieving its objectives. He argued that designers and developers might have difficulty in understanding the required tasks and users. In addition, some tasks and applications with

a variety of different aspects and requirements are complicated to be designed, developed and used which make the application of HCI difficult.

The usability heuristics are very useful to be used for interaction designs in the field of the usability engineering. There are many usability heuristics have been suggested and proposed which can be used as a rule of thumbs which can help in identifying and fixing the common usability issues and problems in the design and associated with the user interfaces in the early stage of the design. However, the results of the heuristic evaluation can be affected by the researcher and cognitive biases. Theses biases can be reduced by involving multiple evaluators and participants in the heuristic analysis and evaluation. In addition, the participants should be provided with a good brief in order to understand the current research and work. Therefore, these aspects will be considered when conducting the questionnaire and focus group sessions.

A number of general usability guidelines are proposed to be used for designing interfaces. In addition, there are several guidelines and principles are introduced by modifying the general principles and concepts to focus on security tools and aspects. Some of the proposed guidelines for each group will be discussed in the following two sections.

6.3 General Usability Guidelines for GUIs

Nielsen (1994) has introduced ten Usability Heuristics for user interface design which have been used in many studies. Nielsen's heuristics are broad rules which are used to recognise and identify any design or usability issues associated with the user interface. These heuristics are proposed to improve usability and address other user interface problems such as inconsistency and complexity. Nielsen (1994) added that the 10 heuristics seem to be effective in providing a useful explanation about usability issues discovered and helping in finding new GUI issues and problems. Nielsen's heuristics are

considered the most used usability heuristics for users interface design (Liyanage, 2016).

Nielsen's Usability Heuristics are presented in Table 6.1.

Criteria of HCI	Description
Visibility of system status	The system should always keep users informed about what is going on, through appropriate feedback within reasonable time.
Match between system and the real world	The system should speak the users' language, with words, phrases and concepts familiar to the user, rather than system-oriented terms. Follow real-world conventions, making information appear natural logical order.
User control and freedom	Users often choose system functions by mistake and will need a clearly marked "emergency exit" to leave the unwanted state without having to go through an extended dialogue. Support undo and redo.
Consistency and standards	Users should not have to wonder whether different words, situations, or actions mean the same thing.
Error prevention	Even better than good error messages is a careful design which prevents a problem from occurring in the first place. Either eliminate error-prone conditions or check for them and present users with a confirmation option before they commit to the action.
Recognition rather than recall	Minimize the user's memory load by making objects, actions, and options visible. users should not have to remember information from one part of the dialogue to another. Instructions for use of the system should be visible or easily retrievable.
Flexibility and efficiency of use	Accelerators unseen by the novice user may often speed up the interaction for the expert user such that the system can cater to both inexperienced and experienced users. Allow users to tailor frequent actions.
Aesthetic and minimalist design	Dialogues should not contain information which is irrelevant or rarely needed. Every extra unit of information in a dialogue competes with the relevant units of information and diminishes their relative visibility.
Help users recognize, diagnose, and recover from errors	Error messages should be expressed in plain language (no codes), precisely indicate the problem, and constructively suggest a solution.
Help and documentation	It may be necessary to provide help and documentation. Any information should be easy to search, focused on the user's task, list steps to be carried out, and not be too large.

Source: (Nielsen, 1994)

Table 6.1: 10 Usability Heuristics for User Interface Design

Chen & MacRedie (2005) revised Nilsen's heuristics and considered three additional principles which were derived from the study of Muller et al. (1998). They argued that the interfaces and the system design should:

1. Support and extend the user's current skills.
2. Pleasurable and respectful interaction with the user.
3. Protect personal information.

Shneiderman & Plaisant (2004) proposed a collection of principles known as "Eight Golden Rules of Interface Design". These rules can be applied and used while designing and developing user interfaces which can provide UI best practices. They are derived from experience after being refined and improved in order to enhance the process of user interface design. Table 6.2 presents the eight golden rules of interface design.

Principle	Explanation
Strive for consistency	Consistent sequences of actions should be required in similar situations; identical terminology should be used in prompts, menus, and help screens; and consistent colour, layout, capitalization, fonts, and so on, should be employed throughout.
Seek universal usability	Recognize the needs of diverse users and design for plasticity, facilitating transformation of content. Novice to expert differences, age ranges, disabilities, international variations, and technological diversity each enrich the spectrum of requirements
Offer informative feedback	For every user action, there should be an interface feedback. For frequent and minor actions, the response can be modest, whereas for infrequent and major actions, the response should be more substantial.
Design dialogs to yield closure	Sequences of actions should be organized into groups with a beginning, middle, and end. Informative feedback at the completion of a group of actions gives users the satisfaction of accomplishment, a sense of relief, a signal to drop contingency plans from their minds, and an indicator to prepare for the next group of actions.

Prevent errors	As much as possible, design the interface so that users cannot make serious errors. If users make an error, the interface should offer simple, constructive, and specific instructions for recovery. Erroneous actions should leave the interface state unchanged, or the interface should give instructions about restoring the state.
Permit easy reversal of actions	As much as possible, actions should be reversible. This feature relieves anxiety, since users know that errors can be undone, and encourages exploration of unfamiliar options.
Keep users in control	Experienced users strongly desire the sense that they are in charge of the interface and that the interface responds to their actions. They don't want surprises or changes in familiar behavior, and they are annoyed by tedious data-entry sequences, difficulty in obtaining necessary information, and inability to produce their desired result.
Reduce short-term memory load	Humans' limited capacity for information processing in short-term memory (the rule of thumb is that people can remember "seven plus or minus two chunks" of information) requires that designers avoid interfaces in which users must remember information from one display and then use that information on another display.

Source: (Shneiderman & Plaisant, 2004)

Table 6.2: Shneiderman's Eight Golden Rules of Interface Design

6.4 Guidelines for Usability in Security Applications

The continuous growth in the information security field has involved human-computer interaction aspects. The usability improvement of security systems becomes an essential task which needs to be considered in order to achieve information security objectives by employing HCI principles. HCISec focuses on the interaction between users and computers in the field of information security. The main objective of HCISec is to enhance security by improving GUI features and components. This can make IT systems more secure, reliable, usable and effective. HCISec mainly highlights and solves the issues between security and usability.

Johnston et al. (2003) have modified Nielsen's HCI criteria in order to be used in the computer security aspects effectively. They have introduced HCISec design principles which can show how the security features of interfaces can be improved in order to be made more easier and user friendly which can help in improving the user experience and make less mistakes. Table 6.3 illustrates the criteria proposed by Johnston et al. (2003).

Criteria	Description
Convey features	The interface needs to convey the available security features to the user.
Visibility of system status	It is important for the user to be able to observe the security status of the internal operations.
Learnability	The interface needs to be as non-threatening and easy to learn as possible.
Aesthetic and minimalist design	Only relevant security information should be minimalist design displayed.
Errors	It is important for the error message to be detailed and to state, if necessary, where to obtain help.
Satisfaction	Does the interface aid the user in having a satisfactory experience with a system?

Source: (Johnston et al., 2003)

Table 6.3: The Proposed HCISec Criteria by Johnston et al

Whitten & Tygar (1999) argued that a different usability standard is required to make security more effective. They stated that the security software could be usable if the main users who are going to use the software are reliably made aware of the required security tasks and are able to know how to successfully do the required tasks without serious errors. They also added that users should be comfortable with the interfaces. Chiasson et al. (2006) reviewed the criteria proposed by Whitten & Tygar (1999) and suggested two additional criteria: users should be informed when their task has been completed and receive good feedback which shows the current state of the system.

Katsabas et al. (2005) reviewed several HCI guidelines which were used for designing user interfaces and applications. They proposed ten HCISec guidelines which need to be followed and considered in order to enhance security features and systems as presented in Table 6.4.

Criteria	Description
Visible system state and security functions	Applications should not expect that users will search in order to find the security tools or have hidden features inside the application. Furthermore, the use of status mechanisms can keep users aware and informed about the state of the system. Status information should be periodically updated automatically and should be easily accessible.
Security should be easily used	The interface should be carefully designed and require minimal effort in order to make use of security features. Additionally, the security settings should not be placed in several different locations inside the application, because it will be hard for the user to locate them.
Suitable for advanced as well as first time users	Show enough information for first time user while not too much information for an experienced user. Provide shortcuts or other ways to enable advanced users to control the software easily.
Avoid heavy use of technical vocabulary or advanced terms	Beginners will find it hard to use the security features in their application if technical vocabulary and advanced terms are used.
Handle errors appropriately	Plan the application carefully so that errors caused by the use of security features could be prevented and minimized as much as possible. However, when errors occur, the messages have to be meaningful and responsive to the problem.
Allow customization without risk to be trapped	Exit paths should be provided in case some functions are chosen by mistake and the default values should be easily restored.
Easy to setup security settings	This way the user will feel more confident with changing and configuring the application according to their needs

Suitable Help and documentation for the available security	Suitable help and documentation should be provided that would assist the users in the difficulties they may face.
Make the user feel protected	Assure the user's work is protected by the application. Recovery from unexpected errors must be taken into account and the application should ensure that users will not lose their data. The user should be provided with the latest security features.
Security should not reduce performance	By designing the application carefully and using efficient algorithms it should be possible to use the security features with minimum impact on the efficiency of the application.

Source: (Katsabas et al., 2005)

Table 6.4. HCISec Guidelines Proposed by Katsabas et al.

Ibrahim et al. (2010) reviewed and analysed more than 10 usability guidelines and criteria including most of the guidelines that already reviewed above. They proposed a further set of HCISec usability criteria with 16 principles for the interface design of end-user security tools. The identified criteria are presented and listed in Table 6.5.

Criteria	Description
Interfaces Design Matches User's Mental Model	Interfaces should be designed and developed based on user's thinking in order to match their mental pattern.
Aesthetic and Minimalist Design	Security alerts should only show the important and relevant information.
Visibility of the Alert Detector Name	It is useful to show the tool name when the alert is displayed.
Establish Standard Colours to Attract User Attention	In information security, the use of red, yellow, orange and green is very useful and can tract the user's attention.
Use Icons as Visual Indicators	The use of pictures and icons in the interface can have a good impact on the user's attention and interaction.
Use Icons as Visual Indicators	The use of pictures and icons in the interface can have a good impact on the user's attention and interaction.
Explicit Words to Classify the Security Risk Level	Information on the security risk level must be displayed clearly in the main interface.

Consistent Meaningful Vocabulary and Terminology	Security information and alerts should be written in a simple and short sentence with enough information and easily understood by users.
Consistent Controls and Placement	Security features and controls need to be placed in a good location in the interface in order to be found easily.
Learnability, Flexibility and Efficiency of Use	Interface and security aspects should be efficient and flexible when users use them. In addition, users should be able and encouraged to learn security knowledge and basics to enhance their awareness.
Take Advantage of Previous Security Decision	Users should be provided with statistical reports and information about their previous security decisions. In addition, user's experience with alerts can be accessed by other users as social feedback in order to help them to make the right decision and increase their learnability.
Online Security Policy Configuration	A default configuration for the security policy can be developed for users in order to guide them to modify their security settings effectively.
Confirm / Recover the Impact of User Decision	The interface should be designed to reduce and prevent users from making errors by providing them with a confirmation message that discusses how the response or decision will affect the security and the system.
Awareness of System Status all the Time	The interface should provide users with a report that shows the status of the system.
Help Provision and Remote Technical Support	The interface or the system should provide users with further support, help and remote support facility to solve any security problem as a final attempt.
Offer Responses that Match User Expectation	The security system should be designed to understand users correctly and achieve their expectations.
Trust and Satisfaction	Users should understand the interface or the system easily and be able to react correctly to security alerts in order to reach a good level of trust and satisfaction.

Source: (Ibrahim et al., 2010)

Table 6.5: HCISec Guidelines Proposed by Ibrahim et al.

After reviewing different general usability guidelines and HCISec principles, it was found that the usability principles proposed by Ibrahim et al. (2010) have covered most of the HCI guidelines. Each principle has a unique purpose and goal which can reduce any conflicts with other principles. Therefore, this guideline will be considered, applied and

used to design and develop flexible usable interfaces that inform and engage users, enabling improved security management and awareness.

6.5 Preliminary Prototypes

A new approach is proposed as an attempt to bridge the current gap and provide home users with an effective tool for managing security across a range of technologies that could be found within the home. The proposed system consists of several components and elements such as the dashboard, the enrolment, the management and the policies. In addition, it includes messages, reports and support sections in order to provide an efficient system.

Several internal rounds of throwing around different ideas and different ways of presenting information by considering the usability principles and guidelines in order to design usable interfaces with effective use of different elements and aspects such as colours, icons and fonts. Two different designs are proposed for each interface in the proposed approach which can be offered to the participant in order to give them more options to select the preferred design for each interface.

Two initial prototypes have been designed and developed in order to test the concept and the process of the proposed approach: low-fidelity and high-fidelity prototypes.

6.5.1 Low-fidelity Prototype

The low-fidelity prototype is a simple way to turn ideas into a testable artefact by using a pen and paper in order to collect and analyse feedback and suggestions in the early stages (Esposito, 2018). Several internal rounds of throwing around different ideas and different ways of presenting information and understating HCI literature and concepts have been conducted. Two different designs are proposed for each component in order to get the

main stakeholders' feedback on them and explore a number of possible options with a view to understanding their preferences in the next chapter and select the most preferred design for each component in order to be used in the final solution.

Figure 6.1 presents two low-fidelity designs which are suggested to be used to simulate the main dashboard in the proposed approach. Each design has different structure and presentation for the information which can be used by the administrator to manage and control the digital devices

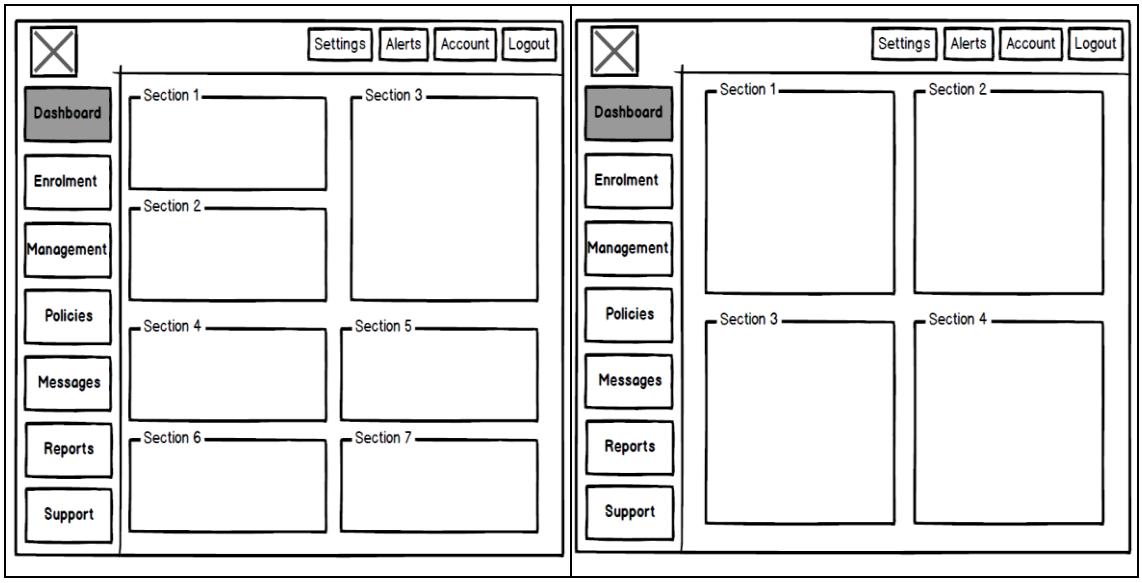


Figure 6.1: Two Low-fidelity Designs for The Main Interface

Figure 6.2 offers two low-fidelity designs which can show the suggested two concepts which can be used to enrol users and devices in the proposed approach. One of the suggested concepts in the design is to enable administrators to drag and drop a specific user and device and the required security policies. The second proposed design is to administrators to click and select the required user, device and security policies.

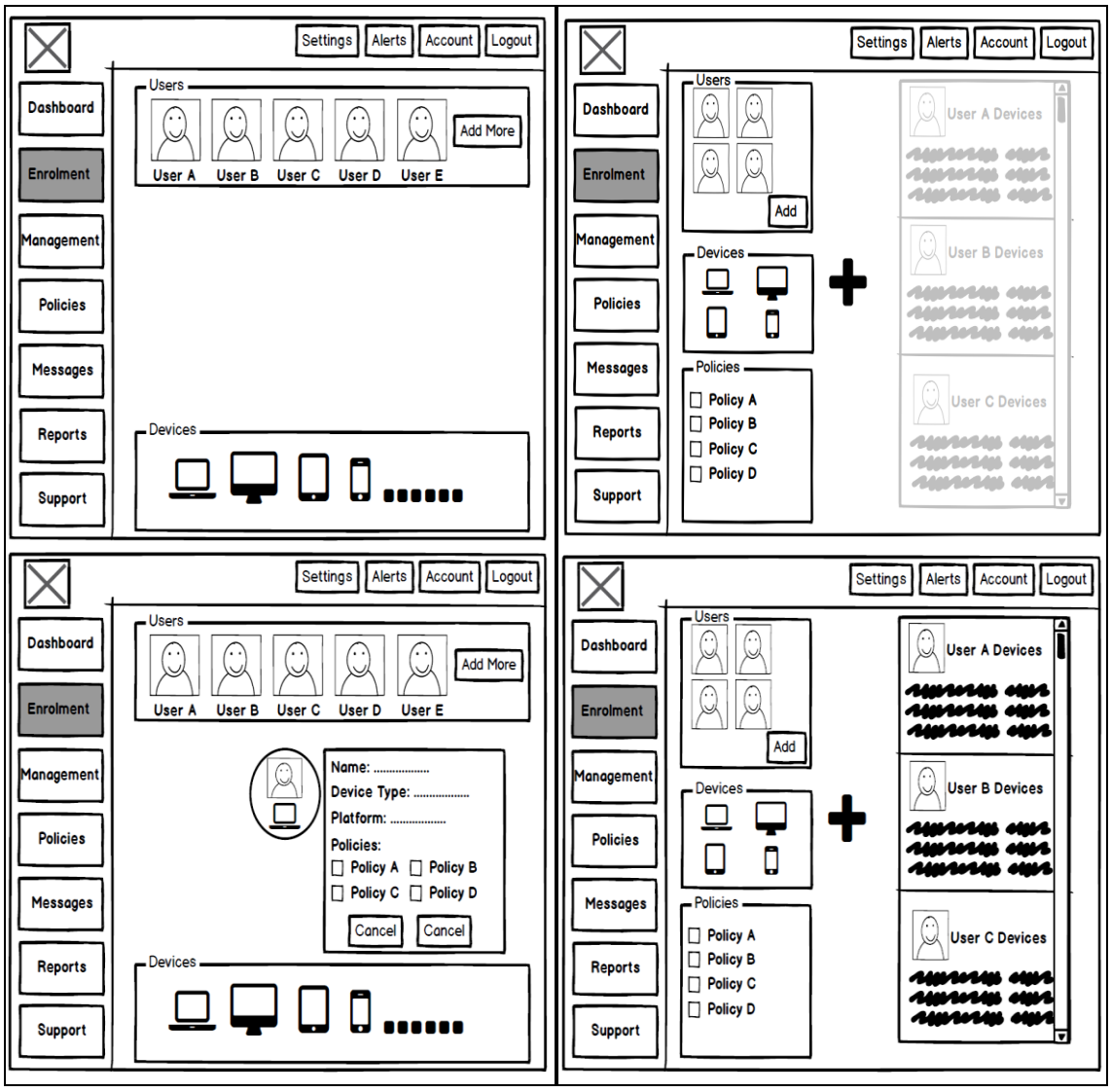


Figure 6.2: Two Low-fidelity Designs for The Enrolment Interface

Figure 6.3 presents two low-fidelity designs which can show how the devices and the users can be managed and presented to the administrator. The first design is to divide the page into two areas: the first side shows compliant devices and the second shows the noncompliant devices. The second design presents all the users and their devices which have been enrolled in the solution in a hierarchical style.

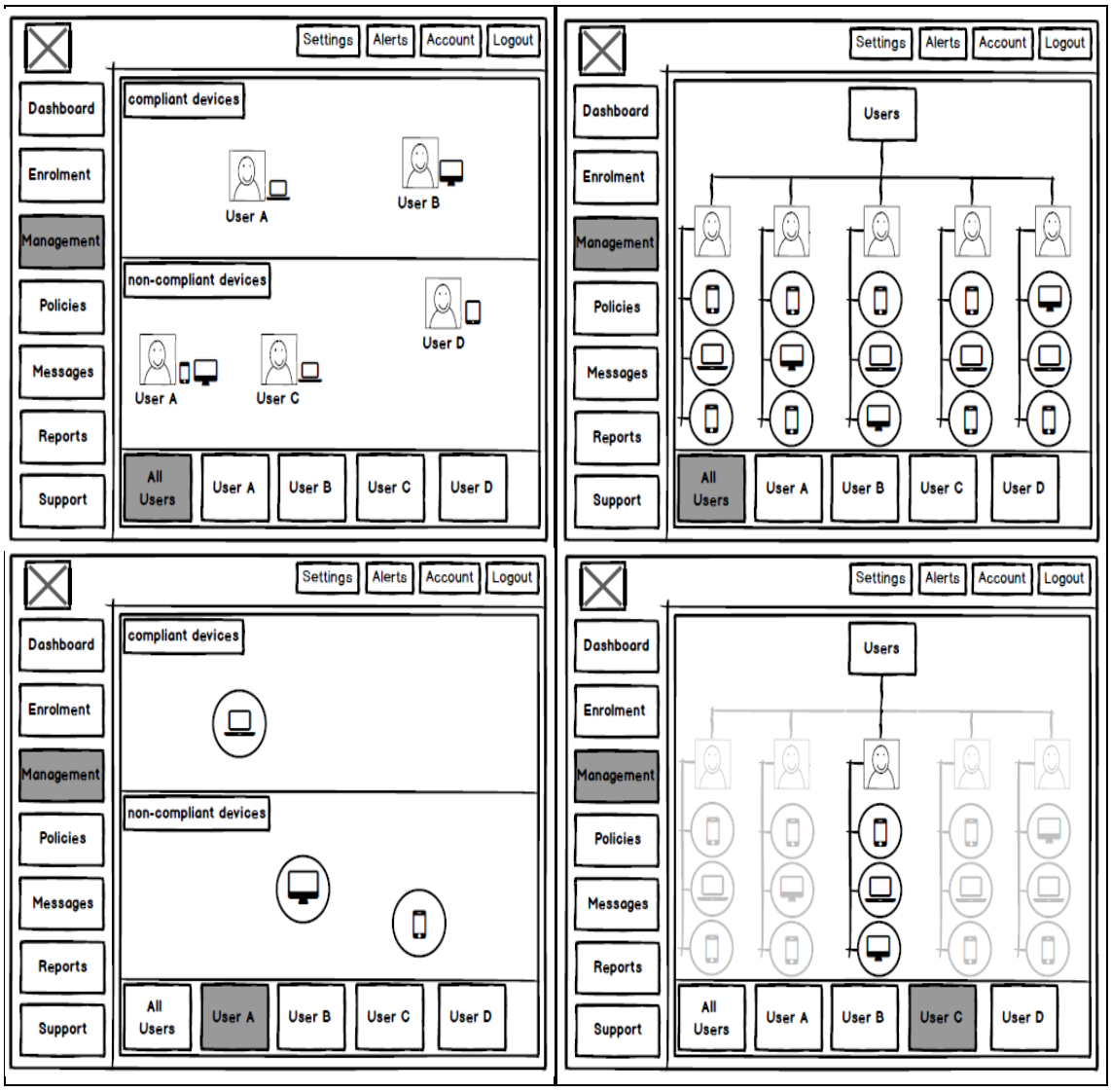


Figure 6.3: Two Low-fidelity Designs for The Management Interface

Two low-fidelity designs are presented in Figure 6.4 which can show two options of presenting and designing the user profile which can be used by the administrator. The first design presents the security policies in a horizontal menu and the second design uses clickable boxes for demonstrating the security policies.

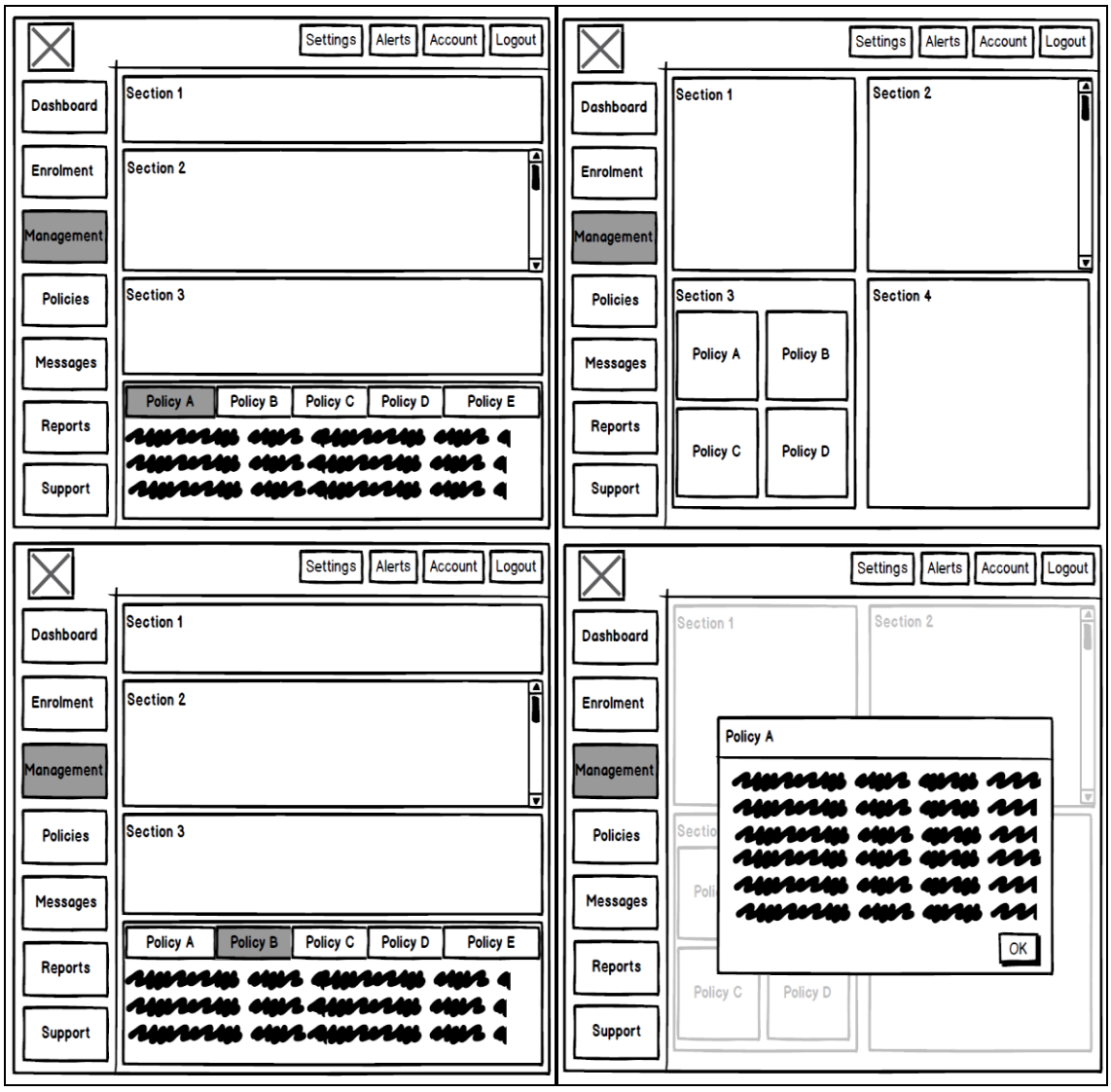


Figure 6.4: Two Low-fidelity Designs for The User Profile

Figure 6.5 presents two low-fidelity designs with two different presentations and layout which can be used for the end user profile in the proposed approach. The first interface is designed as clickable boxes to show the security policies. The second interface is designed as expandable sections which include the security policies.

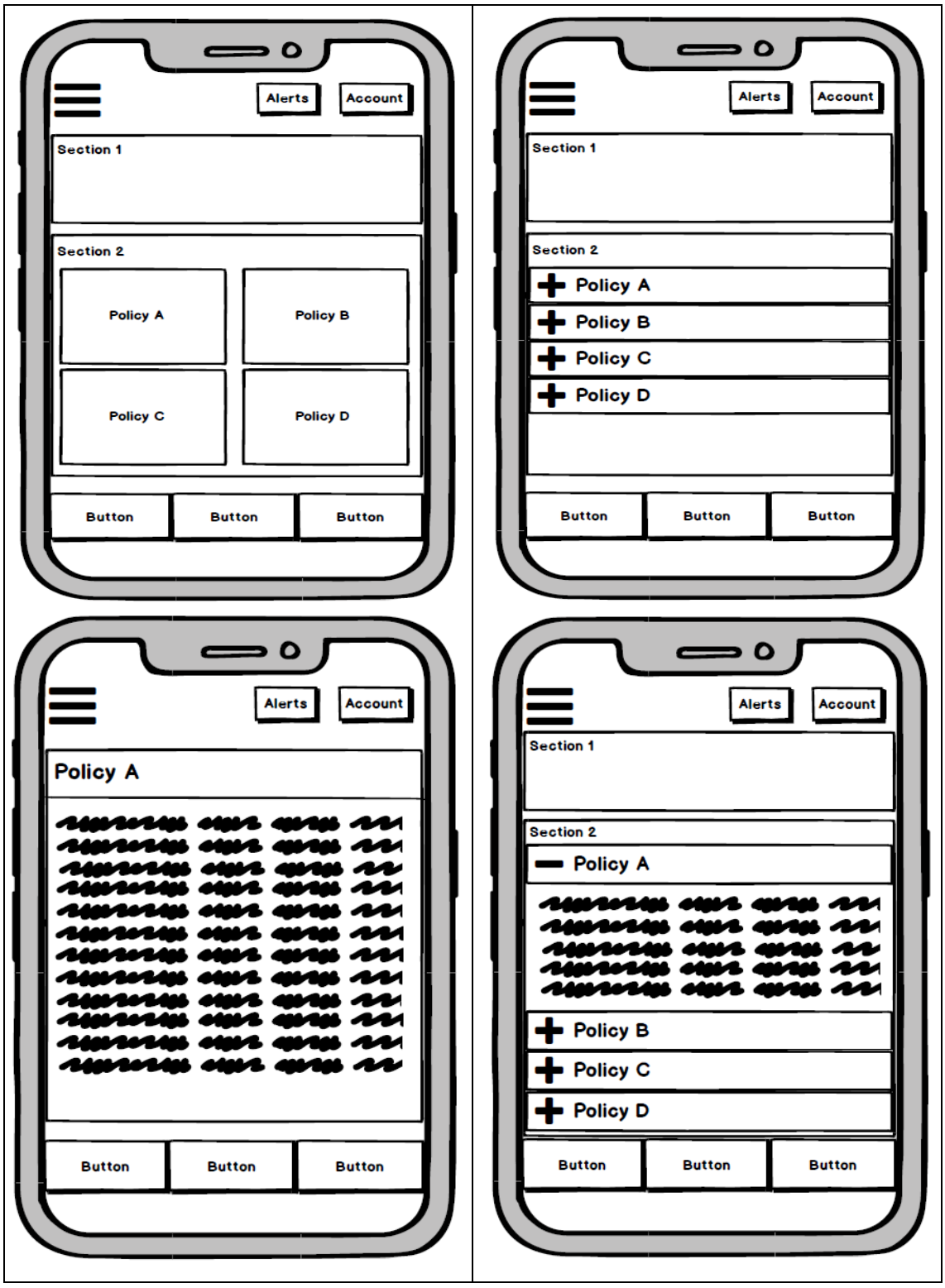


Figure 6.5: Two Low-fidelity Designs for The End User Profile

All the proposed initial low-fidelity designs have been printed out. Several internal sessions have been conducted with some researchers in the research lab at the University

of Plymouth. Theses session helps us in simulating the low-fidelity designs and conducting usability testing in order to gather useful feedback in order to meet user's expectations and improve the solution effectively.

Figure 6.6 shows the paper prototype sessions which have been conducted for simulating and testing the proposed design for the management interface in the suggested approach. Once the user points on "*Users A*", the next interface will be presented to him to simulate the suggested process.

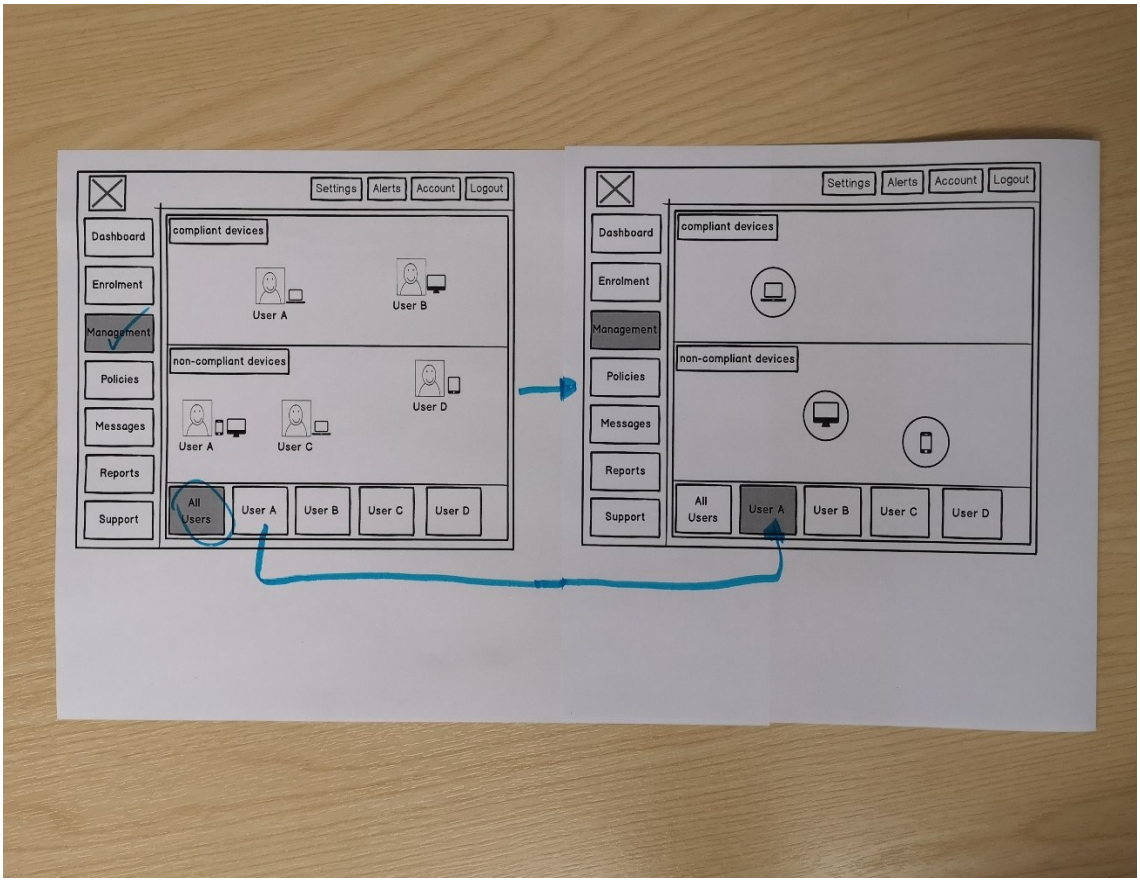


Figure 6.6: Paper Prototype for The Management Interface

Figure 6.7 illustrates the paper prototype session for simulating and testing the proposed design for the user profile interface which can be offered to the administrator in the suggested approach. Once the user points on "*Policy A*", the next interface will be shown

to the user with more detail about the required policy in order to simulate the suggested process and concepts.

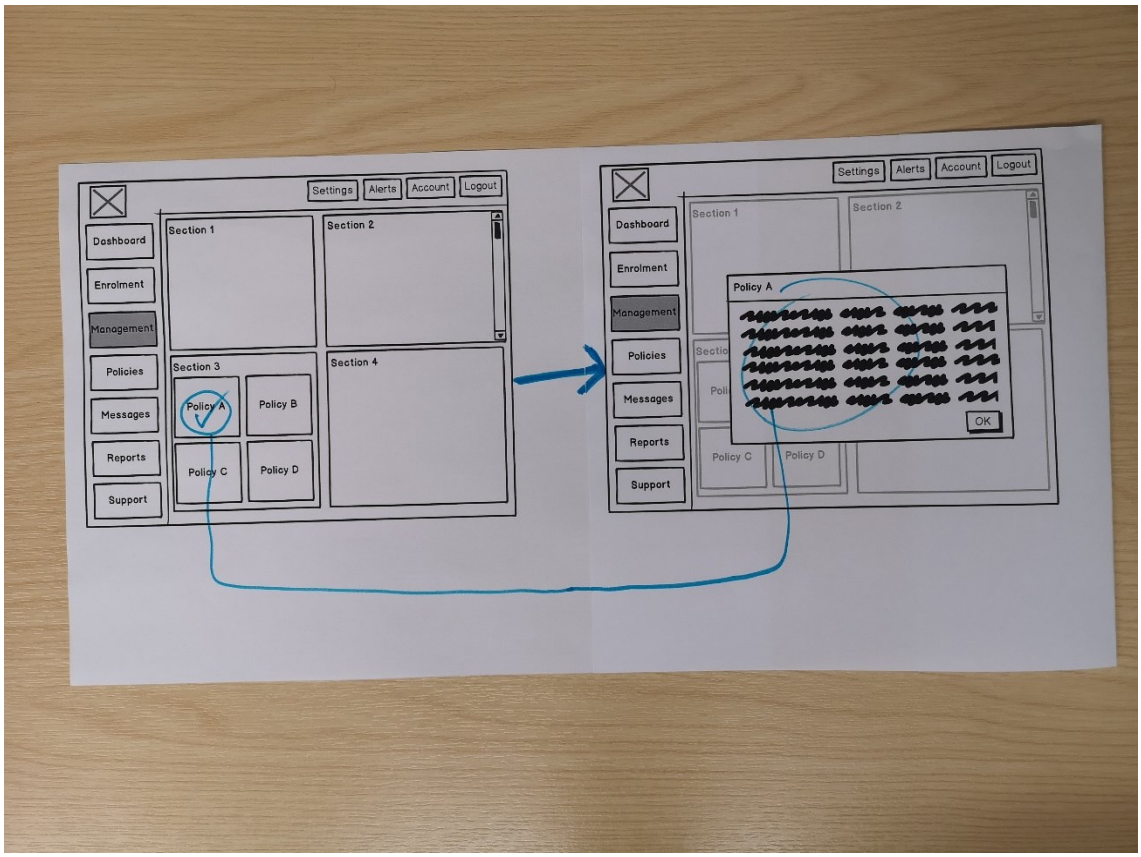


Figure 6.7: Paper Prototype for The User Profile for The Administrator

The paper prototype for simulating and testing the proposed design for the user profile interface is presented in Figure 6.8. The profile interface can be used by the end-users in the suggested approach. Once the user selects and clicks on "*Policy A*", the next interface will be shown to the user with more detail about the required policy in order to simulate the suggested process and concepts.

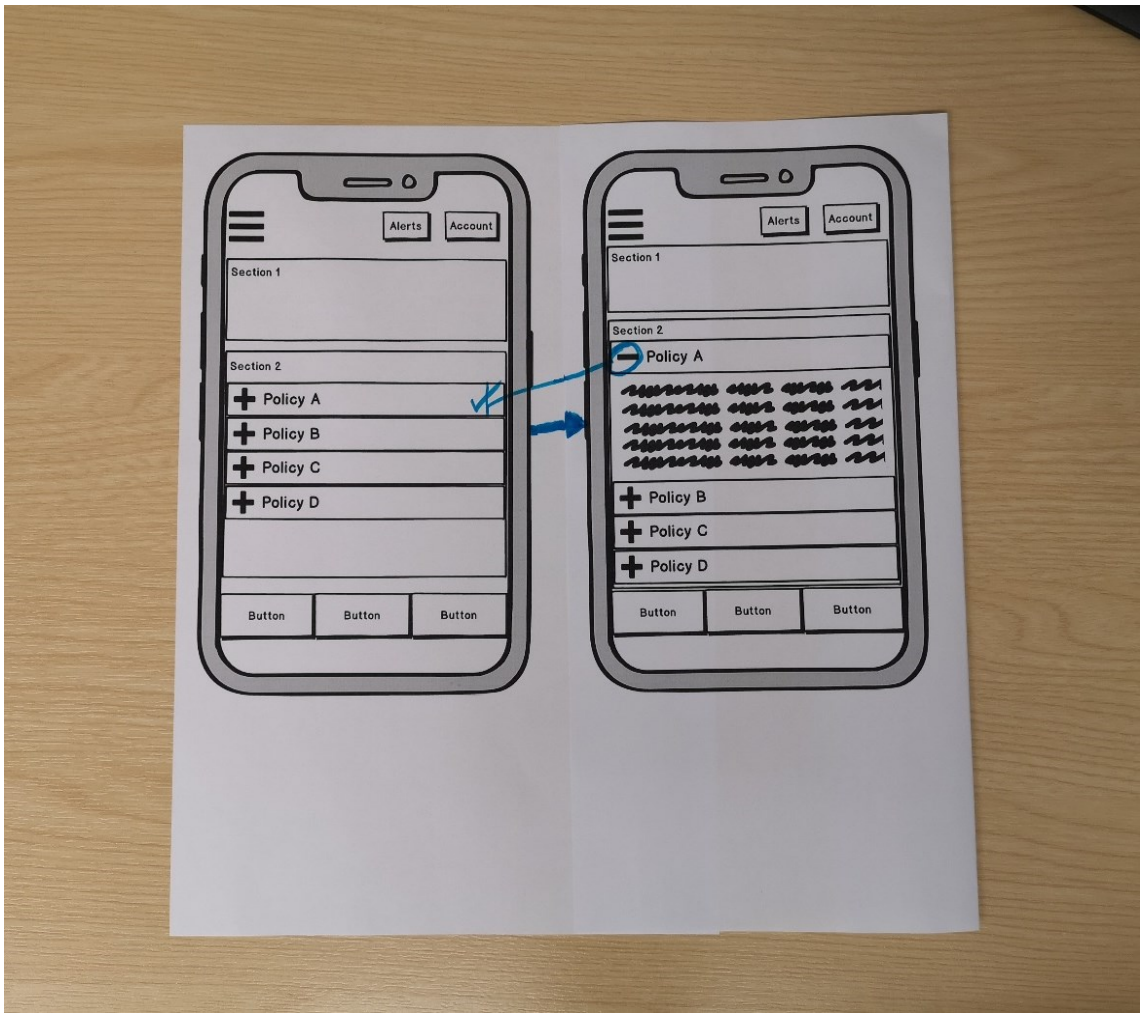


Figure 6.8: Paper Prototype for The End User Profile

Some comments and feedback about the navigation, contents and the structure have been collected and gathered by undertaking some initial testing with the paper prototypes for the proposed designs. The paper prototypes can help us in improving the proposed approach and moving into high-fidelity designs effectively which will be presented in the next section.

6.5.2 High-fidelity Prototype

After proposing, designing and testing low-fidelity interfaces for the proposed approach, all the low-fidelity interfaces are converted into high-fidelity interfaces by considering different HCI criteria and principles. Moqups app web is selected to develop a digital

high-fidelity prototype which can provide clickable objects and interactions in order to show and visualise the process and the concepts of the propped approach.

The following sections discuss the proposed high-fidelity interfaces for several components and elements in the proposed approach such as the dashboard, the enrolment, the management and the policies.

6.5.2.1 The Main Dashboard (for Administrators)

The main aim of the dashboard is to notify the administrator in a good method about different security aspects and statistical information. Two initial interfaces were designed for the main dashboard with different structure, presentation and information.

In the interface designs for the whole system, the main menu, system alerts and other controls such as user accounts, logout and settings option are placed on the left side and top side of all the proposed interfaces which can be considered as a good location for security controls and features. This can help users to use the system and its features easily as recommended by Ibrahim et al. (2010).

In addition, a bell alarm icon is used to represent the security alerts for the whole system as shown in the below figures. The number of security issues will be displayed in a red box in order to attract user attention. More information about the detected threat or issue can be provided to users when they click on the bell icon. The use of icons and red colour can make the interface easily used as recommended by Ibrahim et al. (2010). In addition, the system alerts can keep users informed and aware about the system status and what is going on as this criterion is suggested by Ibrahim et al. (2010).

The main menu is designed and supported with images for each section in order to be distinguished easily by users. The current selected section in the menu will have a dark

background in order to be recognized easily by users. the use of icon feature is also recommended by Ibrahim et al. (2010) as they suggested to use icons as visual indicator and recognition.

The proposed approach can be hosted online as a web-based application in order to be available accessed by the main stakeholders all the time. Once the users (administrators and end-users) access the application, they will be provided with a login page to enter their username and password.

6.5.2.1.1 The First Proposed Design

As shown in Figure 6.9, the icons have been used in different sections in the interface in order to help users to recognize each task and section easily. Each icon and image have been selected and used to describe the related sections and tasks in order to use the system easily as recommended by Ibrahim et al. (2010).

Figure 6.9: The First Proposed Design for The Main Dashboard

The colours used in the interface are selected to highlight the current status, threats or issues. For example, red is used to represent any hazards or current issues while the green colour indicates that a user or device does not have any major security issues. The use of these colours is useful to attract user attention easily and recommended by the HCI guidelines proposed by Ibrahim et al. (2010).

6.5.2.1.2 The Second Proposed Design

In the second proposed design for the main dashboard, the use of red and green colours, which already used in the previous interface, is used to make users aware of threats and issues. The interface provides different data and presentations. The icons and images are

used to represent different users, technologies and digital devices in order to easily identified by users as shown in Figure 6.10.

Figure 6.10: The Second Proposed Design for The Main Dashboard

6.5.2.2 The Enrolment Interface (for Administrators)

The administrator can start the process of the enrolment for adding new users and devices by creating new profiles including users, devices and security policies. Two different design interfaces are proposed for the enrolment process with two different approaches.

6.5.2.2.1 The First Proposed Design (Drag-and-Drop Approach)

This interface is designed by using the feature of Drag-and-Drop technique as illustrated in Figure 6.11. The administrator will be asked to select a user and a device by grabbing

and dropping them blue area. This can make the system easy to use by providing the administrator with only the needed information for the enrolment such as users and devices in order to achieve aesthetic and minimalist design criteria recommended by Ibrahim et al. (2010).

Figure 6.11: The First Proposed Design for The Enrolment

In addition, a confirmation message is provided in the interface to review the enrolment information and the security impact before the final enrolment. This can help administrators to handle and recover errors appropriately in the interface to allow the enrolment and security impact to be reviewed as recommended by Ibrahim et al. (2010).

6.5.2.2.2 The Second Proposed Design (Point-and-Click Approach)

The second proposed interface is designed by utilising the approach of Point-and-Click as illustrated in Figure 6.12.

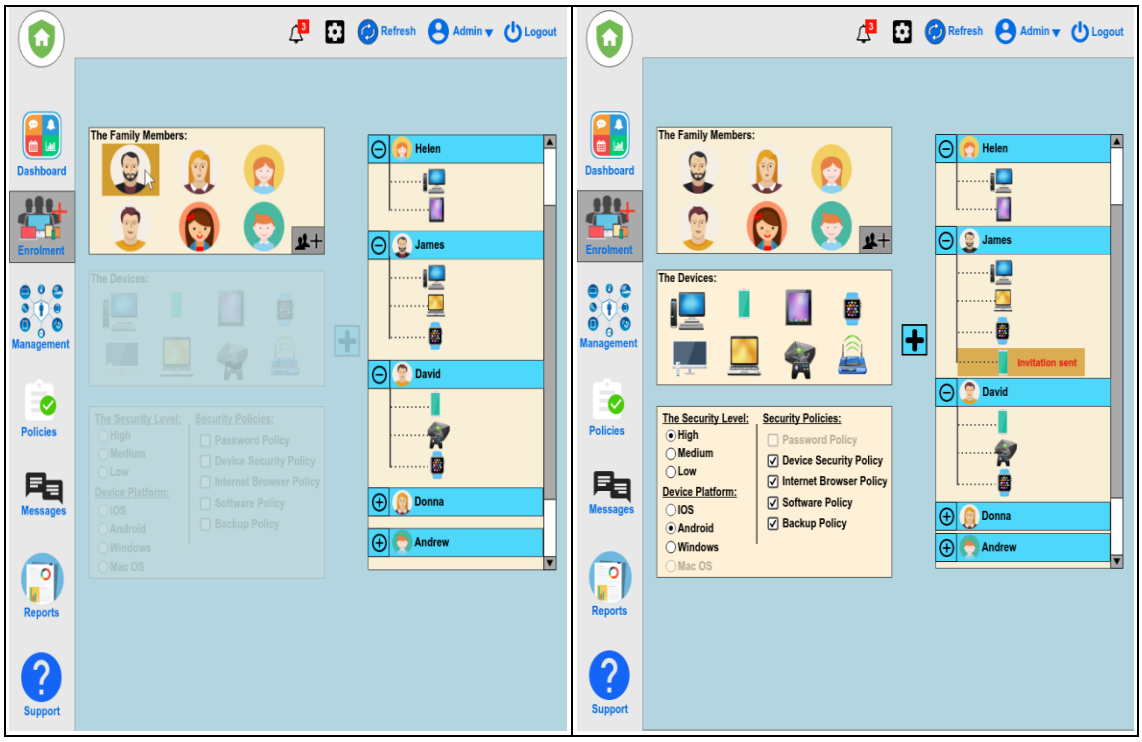


Figure 6.12: The Second Proposed Design for The Enrolment

This approach can make the enrolment setup organized and sequenced in order to provide an easy setup security enrolment as recommended by Katsabas et al. (2005). In addition, this type of approach might enhance and improve user experience and make them satisfied with the enrolment process in order to meet the satisfaction criteria suggested by Ibrahim et al. (2010). In addition, the interface will present a summary enrollment information to allow the administrator to review and confirm the selected settings and policies in order to avoid any mistakes or errors.

6.5.2.3 The Management Interface (for Administrators)

The management section is responsible for managing, monitoring and checking the compliance of the enrolled devices with their assigned policies. Two interface designs were proposed for the management interface with two different presentations and layouts

6.5.2.3.1 The First Proposed Design (Red and Green)

The first proposed interface is designed by providing two areas and utilising the use of red and green colours. The red area represents the non-compliant devices and the green area for the compliant devices as shown in Figure 6.13.

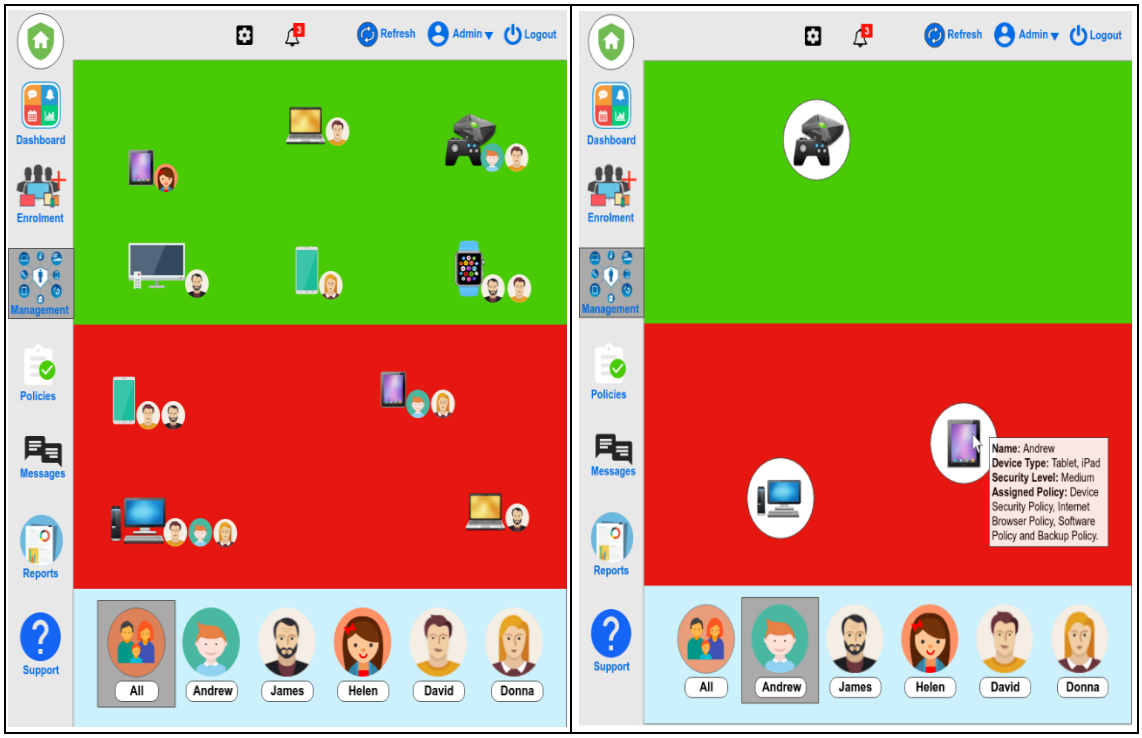


Figure 6.13: The First Proposed Design for The Management

This can help in recognizing the users and their devices whether they have an issue or not. In addition, when the administrator moves a cursor over a specific device, an information box with more information about the status of the device will be shown. This approach can help in meeting the aesthetic and minimalist design criteria recommended by Ibrahim et al. (2010).

6.5.2.3.2 The Second Proposed Design (Hierarchical Style)

The second interface is designed based on a hierarchical style which can give a comprehensive overview and management for all the enrolled devices: the use of red and

green colours is also used as the non-compliant devices have a red circle and the compliant devices have green as presented in Figure 6.14. this approach design would improve the flexibility, efficiency of use and satisfaction as suggested by the HCI guideline proposed Ibrahim et al. (2010).

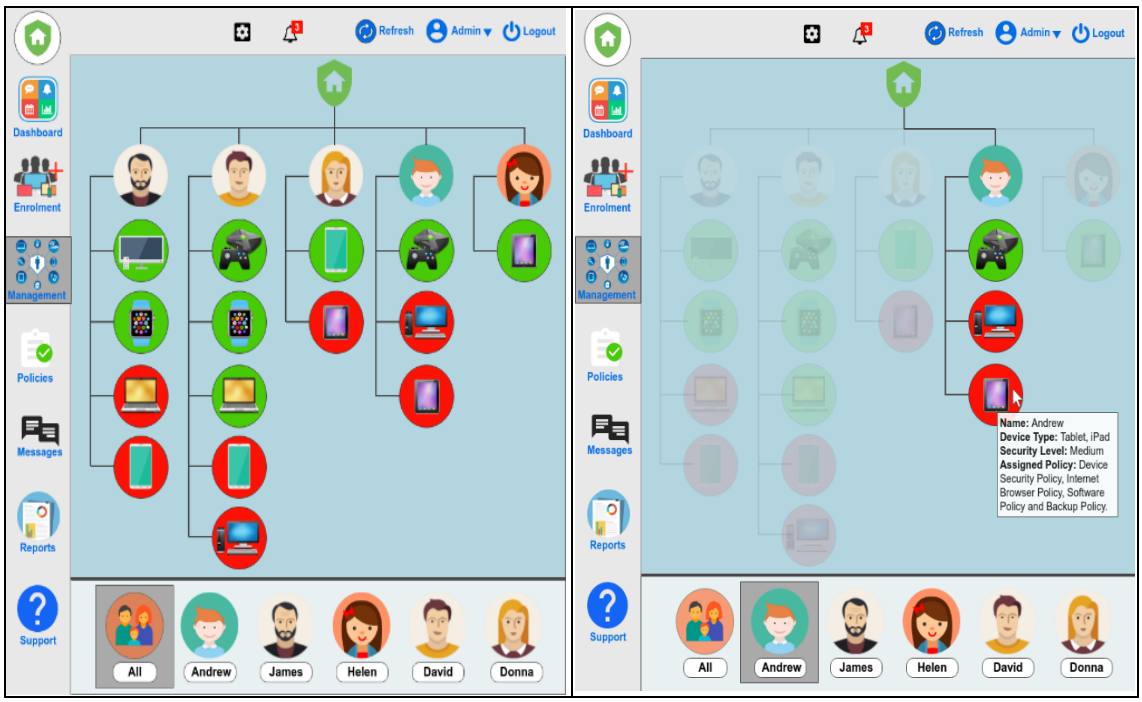


Figure 6.14: The Second Proposed Design for The Management

6.5.2.4 User Profile (for administrators)

Once the administrator clicks on the option of viewing profile in one of the previous interfaces, a comprehensive detail about the status of the device compliance will be provided in a usable way. Two interface designs with different structures and layout are proposed for the user profile interface.

6.5.2.4.1 The First Proposed Design (Horizontal Menu)

The user profile interface is designed to provide the administrator with the required information about a specific user or device. A ring bell icon with a red box is placed at

the top of the interface which highlights the number of alerts or notifications related to a specific device as shown in Figure 6.15.

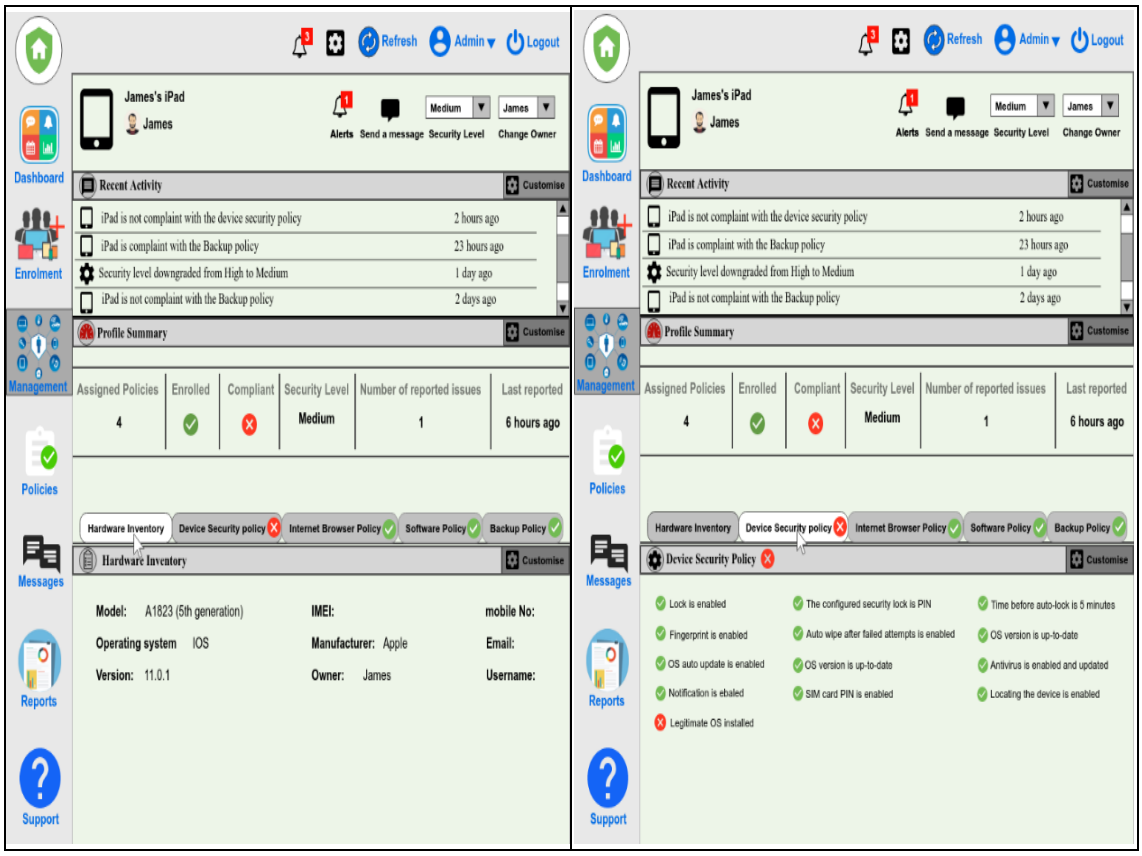


Figure 6.15: The First Proposed Design for the User Profile (Administrators)

In addition, red cross and green check icon are used in different places in the interface to show the current status. The utilization of the colours and icons can support users in identifying and recognizing the current issues easily as advised by HCI guidelines. In addition, the assigned security policies are designed and placed in a horizontal menu with red and green icons to assist the administrator which can improve user experience and satisfaction.

6.5.2.4.2 The Second Proposed Design (Clickable Boxes)

The second interface is designed to show the security policies in clickable boxes. The red and green colours are used in these boxes in order to attract administrator attention as presented in Figure 6.16.

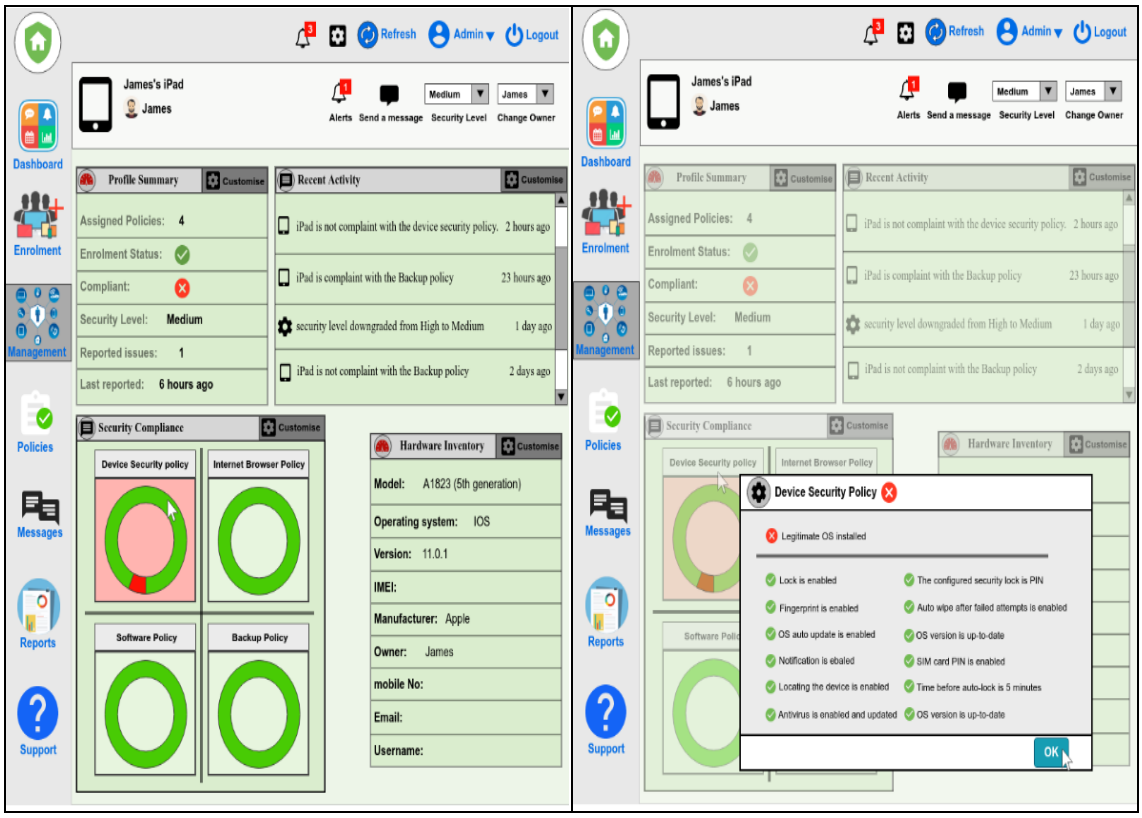


Figure 6.16: The Second Proposed Design for the User Profile (Administrators)

More information about a specific security policy can be provided to the administrator by clicking on a specific box. This can ensure that the interface only shows the relevant and the required information without displaying irrelevant or rarely needed information in order to an aesthetic and minimalist design as recommended by Ibrahim et al. (2010).

6.5.2.5 User Profile (for End-users)

The main duty of the end-user profile is to provide end-users with some security information and a summary of the security status of their enrolled device. In addition, it notifies end-users about their compliance with assigned policies. Two proposed interfaces

are designed for end-user profile interface. The red and green colours are used in the two interface designs to reflect the user compliance with each policy. In addition, a bell icon. green check and red cross icon are used in the interface to show the current status and issues. The use of colours and icons can help end-users to recognize and pay attention to current alerts or issues.

In the two designs, the information security alerts and policy statements are delivered with consistent meaningful vocabulary and simple sentences as recommended by Ibrahim et al. (2010). In addition, a tooltip box appears when users hover the pointer over each policy statement which can provide more information about the current security statement and tips on how to enhance it. This can ensure that end-users are able and encouraged to learn security knowledge and increase their learnability as suggested by the HCI guidelines proposed by Ibrahim et al. (2010).

6.5.2.5.1 The First Proposed Design (Clickable Boxes)

The first interface for end-user profile is designed in clickable boxes with red or green colours in order to attract end-users attention and recognize issues with each policy as shown in Figure 6.17. This can make the interface usable and efficient to use. In addition, the use of clickable boxes can ensure that end users are not offered too much and irrelevant information which can make them confused and make the interface difficult to use.

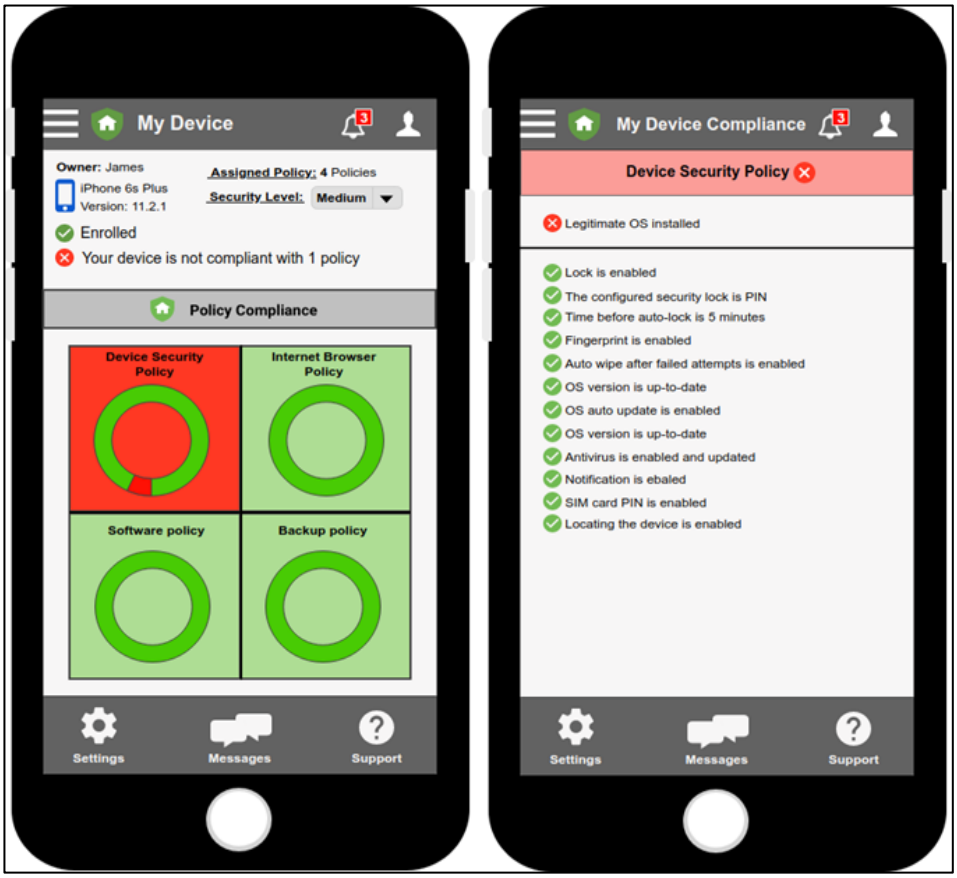


Figure 6.17: The First Proposed Design for the User Profile (End Users)

6.5.2.5.2 The Second Proposed Design (Expandable / Collapsible Sections)

The second user profile interface is designed to deliver present the assigned security policies in expandable/collapsible sections as illustrated in Figure 6.18. This approach can allow end-users to use and interact with the interface components and move between the sections easily.

Figure 6.18: The Second Proposed Design for The User Profile (End Users)

6.6 Summary

The chapter has reviewed the current human-computer interaction criteria and guidelines which are recommended to be considered when designing user interfaces in order to develop flexible usable interfaces. A number of preliminary interfaces are proposed and designed in order to visualizse for the main components and elements of the proposed framework for improving information security management and awareness for home users. Further feedback about these preliminary interfaces will be received by conducting a questionnaire in order to improve and enhance the interfaces in the final design. The questionnaire design and the results will be discussed in the next chapter.

Chapter Seven

An Analysis of Quantitative Results

7 An Analysis of Quantitative Results

7.1 Introduction

The aim of this chapter is to assess information security awareness and management for home users. The questionnaire seeks to understand and investigate the users' concerns, knowledge and management regarding different digital services and security issues. In addition, the questionnaire is conducted to get end-users' feedback about the proposed interface designs in terms of the usability and functionality aspects in order to improve them in the final design. A discussion section will be provided to highlight the main finding and the acceptability of the proposed ideas from the end-user perspective.

7.2 Design and Methodology

The aim of the questionnaire is to measure and evaluate the cyber security concerns, knowledge and management for home users. In addition, it was used to get feedback about the requirements and initial interface designs for the proposed system. The questionnaire for this study has been developed according to the steps shown in Figure 7.1.

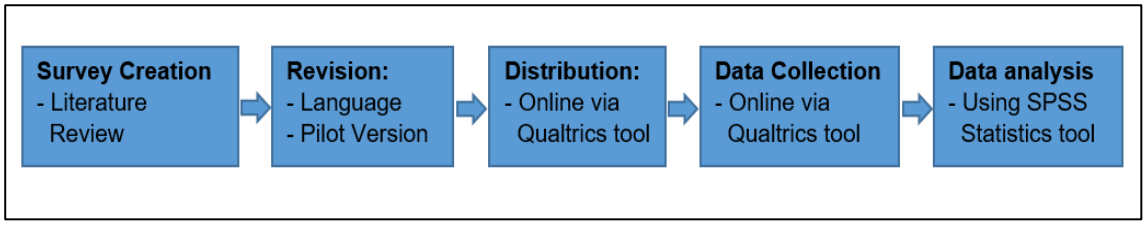


Figure 7.1: The Steps Taken for Conducting The Survey Study

7.2.1 The questionnaire structure

Bowling (2005) states that it is very important that the questions should be very clear in order to make it easy for the respondents to understand the questions and improve the response quality. The questions have been structured as follows (See Appendix A):

- The first part includes classification questions to determine some demographic information, such as gender, age, qualification levels and IT experience levels. These demographic questions can help in analysing the impact of these factors and aspects in order to understand the users online behaviour which can be used and applied in the proposed framework.
- The second part contains different groups with different questions perception questions to determine and understand the level of the stakeholder's concern, knowledge, management and how easy the participants manage the different security controls and configurations which have been reviewed, identified and proposed in chapter 5 by reviewing the best recommended best practices for SMEs and home networks:
  - Security and safety for all the digital devices used by the participants.
  - Security and safety for all the digital devices used by the family members.
  - Password security settings.
  - Antivirus software settings.
  - Operating system security settings.
  - Internet browser security settings.
  - Backup configuration settings.
  - Applications security and management in digital devices.
  - Security configuration of the access points (modem).
  - Parental control settings.
- The third part consists of several points related to the proposed approach to understand and determine the level of agreement of the stakeholders about the following aspects:
  - Applying different levels of security settings the digital devices (such as low, medium and high level)

- The implementation of different security settings should be focused upon the user rather than the device.
- Applying one security level on all the devices which belong to one user.
- Providing pre-defined templates of security settings for users.

- The fourth part has a number of different interface designs are proposed in order to get the feedback of the stakeholders in terms of the following aspects: the structure, the use of colours, text, icons, the coherence of the appearance, the sequence of the sections, the understanding of the interface purpose, the ease of use, the relevance of the information. In addition, the participants are asked which interface design they prefer for each component.

7.2.2 Validation of the questionnaire

A pilot study is considered as a trial to the main study which can be conducted in the research in order to improve efficiency (Teijlingen and Hundley, 2001; Leon *et al.*, 2011; In, 2017). It helps the researcher to find out whether the proposed approach and study used in the research would help to get reliable and accurate results. In addition, any potential problems can be identified and discovered during the pilot study in order to apply an appropriate adjustment before starting the main study. Two pilot tests have been conducted:

- The first pilot test was conducted on 14th August 2018 with a group of participants who are considered to be home users with different educational backgrounds.
- The second pilot test for the survey was conducted on 17th August 2018 with 8 researchers were from the University of Plymouth (4 participants from the Centre for Security, Communications and Network Research (CSCAN) at the university and 4 researchers from different areas: mathematics, biology, education and business.

Participants from diverse backgrounds have been invited to participate in the two pilot studies in order to validate whether the survey is understandable and clear for the participants with different backgrounds. The pilot test sessions have been organized individually and each participant was asked to start answering the questionnaire online. Feedback and suggestions about the questionnaire's aspects have been collected and recorded.

Each participant took around 25 minutes to complete the survey. Common feedback received from the vast majority of the participants was that the survey was long and it should be shorter and simpler. Therefore, the total number of the questions were reduced from 36 to 24 in the survey. Overall, the majority of the participants were able to answer and understand most of the questions in the survey. However, some of the participants experienced some difficulties in understanding some information. Therefore, some questions were modified by using simple terms and definitions in the survey in order to be easily understood and answered. In addition, Minor suggestions and changes were collected from the two pilot tests in terms of language and structure which can make the questionnaire easier to be understood and answered.

7.2.3 Target Participants

The target group of this survey is home users as the proposed framework is for improving the cyber security awareness for home users. The number of participants was expected to reach 400 participants from different countries as similar studies in the same subject such as Talib et al (2010) Al Abdulwahid et al. (2015). In addition, having this number of participants can ensure reliable collected responses and results.

The questionnaire is designed for participants who are above 18 years of age (both genders) over different backgrounds, qualifications and experience. Respondents were

informed on the first page of the survey that taking part in the survey is voluntary and their participation would be kept confidential in compliance with ethical approval rules (See Appendix B).

7.2.4 Responses types

In this survey, all the provided questions were open-ended questions which need to be answered in accordance with the perceptions of the participants. The Likert-type scale, which is developed by Dr Rensis Likert at the University of Michigan, is one the most common tools used for assessing the opinion of the respondents (Saunders et al., 2009). Therefore, the participants were asked to measure their opinion and views about different aspects and items in the questionnaire on a Likert-type scale, 5 points ranging from 1 to 5 as the following:

- **Questions about security concerns:** extremely concerned, moderately concerned, somewhat concerned, slightly concerned and not concerned at all.
- **Questions about security knowledge:** extremely knowledgeable, moderately knowledgeable, somewhat knowledgeable, slightly knowledgeable and not knowledgeable at all.
- **Questions about security management:** always, very often, sometimes, rarely and never.
- **Questions about the ease of managing security:** extremely easy, somewhat easy, neither easy nor difficult, somewhat difficult and extremely difficult.
- **Agreement questions:** strongly agree, somewhat agree, neither agree nor disagree, somewhat disagree, strongly disagree.
- **The assessment of different aspects of the initial interfaces:** excellent, very good, good, fair, poor.

7.2.5 Conducting the questionnaire

An online distribution technique was used in the study in order to cover the required sample size (approximately 400 participations). The questionnaire was conducted via Qualtrics website. This web survey tool facilitates the distribution of the questionnaires with an appropriate link or QR code. In addition, it helps to monitor the received participation and provide the researcher with an initial report. The questionnaire was distributed via e-mail targeting students, staff and colleagues at the University of Plymouth. In addition, social websites and applications were used to reach more participants.

7.2.6 Reducing Bias in The Questionnaire

Several steps and procedures have been undertaken in order to minimise sampling, response, nonresponse and order bias in the questionnaire:

- Sampling Bias: different methods have been used to share and distribute the questionnaire as discussed in the previous section. your survey via various methods. This can help in sharing the survey in such a way that all people have a chance of responding to the survey.
- Nonresponse Bias: an information sheet that explains the aim of the survey has been sent to the respondents. In addition, a reminder has been sent to the respondents who did not confirm that they completed the survey.
- Response Bias: the questionnaire has been conducted online which can make the questions self-administered which can reduce the potential for response bias. In addition, the respondents have been informed that their participation is kept anonymously.

- Order Bias: different groups of questions with different topics have been included in the questionnaire. In addition, the questions have been made as engaging as possible in order to the question order research bias.

7.2.7 Data Analysis

Statistical Package for the Social Sciences (SPSS) is one of the most popular statistical tool used by researchers to get an advanced statistical analysis in the social and behavioural science (Bryman, 2016). All the data analysis were conducted by using IBM SPSS Statistics for Windows, Version 24.0. Qualtrics has an option to export all the completed responses and participations as a numerical format in a CSV file. This makes transferring the collected data from the website to SPSS very easy and fast. The following two tests have been conducted to get more analysis:

1. Pearson's coefficient correlation test

Pearson's coefficient correlation test is one of the most popular techniques for measuring the correlation between two factors (Price, 2000). In this study, the two-tailed Pearson's coefficient correlation test was used to measure the significance level of Pearson's correlation. The Sig (2-Tailed) value can tell the researcher if there is a statistically significant correlation between your two variable or not:

A. If the Sig (2-Tailed) value is greater than 0.05, it can be concluded that there is no statistically significant correlation between your two variables.

B. If the Sig (2-Tailed) value is less than or equal to 0.05, it can be concluded that there is a statistically significant correlation between your two variables.

In addition, the correlation value (r) is always between -1.0 and +1.0. If the r is close to 1.0 or -1.0, it indicates that there is a strong correlation between the two variables.

However, if the correlation equals 0, it means the there is no correlation between the two variables as shown in Table 7.1 (Hinkle et al, 2003).

Correlation Size	Interpretation	Correlation Size	Interpretation
.90 to 1.00	Very high positive correlation	-.90 to -1.00	Very high negative correlation
.70 to .90	high positive correlation	-.70 to -.90	high negative correlation
.50 to .70	Moderate positive correlation	-.50 to -.70	Moderate negative correlation
.30 to .50	Low positive correlation	-.30 to -.50	Low negative correlation
.00 to .30	Negligible correlation	-.00 to -.30	Negligible correlation

Source: (Hinkle et al., 2003)

Table 7.1: Rule of Thumb for Interpreting the Size of a Correlation Coefficient

2. One-way analysis of variance (ANOVA)

One-way ANOVA is a statistical method used to measure the statistical difference between two variables (Quartey, 2003). One-way ANOVA is widely used for analysing quantitative data. It is mainly used to determine whether there are any statistically significant differences between the means of two or more independent groups (Malhotra et al., 1999). The F ratio indicates the difference between the groups. The smaller the F ratio, the smaller is the difference between the groups. However. If the F ratio is large, the difference between the groups is likely to be more statistically significant (Cramer and Howitt, 2004). The one-way ANOVA test was used in this study to measure whether there is a statistically significant difference between some groups or not in some responses.

In addition, the arithmetic mean equation measured and calculated by using the SPSS in order to identify the central tendency of the responses in order to provide better interpretation for the results.

A thematic analysis was chosen as a method for analysing the comments collected from the questionnaire. It is the most popular method used to analyse qualitative data. Silver and Lewins (2014) stated that this method can help in exploring and analysing the collected qualitative data by proposing several themes which can be derived from the research questions. Several steps were suggested by Braun and Clarke (2006) and Saunders et al. (2009) used in analyzing the collected comments:

- Preparing and organizing the collected comments and making notes and header for some of the comments.
- Predetermining and generating initial codes that can be developed after reading the collected data.
- Searching for themes: this can be done by reading the text several times. Next, several sections and parts can be identified in the text. In addition, significant and important texts can be interpreted. In addition, the text can be categorised into several themes by merging and combing the related text into the appropriate theme.
- Reviewing, checking and finalising the themes and the finding.
- Defining and naming themes which can present the analysis.
- Producing the report which should provide sufficient evidence of the themes within the data.

7.3 The Results Analysis

This section presents details of the survey that was conducted to investigate the security concerns, knowledge, and management for different security aspects. In addition, it discusses the feedback received from the participants about the initial proposed interfaces which were designed for the suggested approach

In total, 1038 responses have been received during 8 weeks: 434 completed responses and 604 incomplete participations.

7.3.1 Demographic

The analysis of the survey shows that around 71% of the participants are males (311 participants) whilst the remaining respondents are females (132 participants). Participants' age is divided into 5 categories where 93% of the participants are within the age range between 18 and 44 years. As can be seen in the graph below (see Figure 7.2), 69 participants have an age between 18-24 years (16%) and 188 participants have an age between 25-34 years of age (43%). 148 participants have an age between 35-44 years (34%). Only 27 participants are within the age range between 45 and 54 years (6%) and finally 2 participants are 55 years old or older.

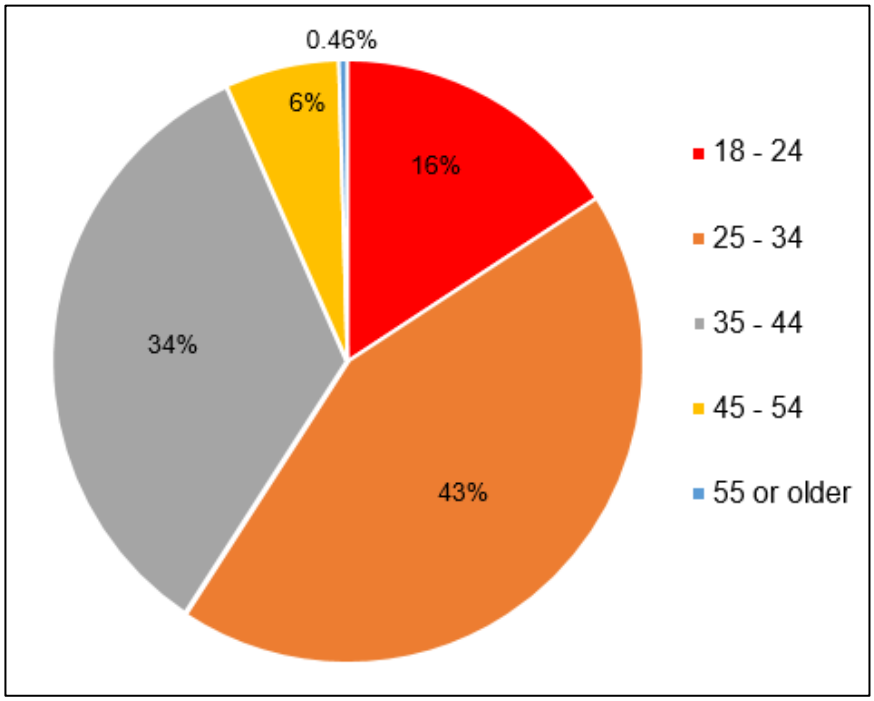


Figure 7.2: Percentages of Participants across Age Groups

The questionnaire also asked about the education level achieved by the participants which are divided into 5 categories. 191 participants (44%) have a postgraduate degree (either a

Master or a PhD degree) and 183 participants hold a bachelor's degree (42%). Only 22 participants have a college certificate (5%) and 35 participants have high school qualifications (8%). Overall, it can be observed that 86% of the participants have a qualification at the undergraduate level or higher as shown in Figure 7.3.

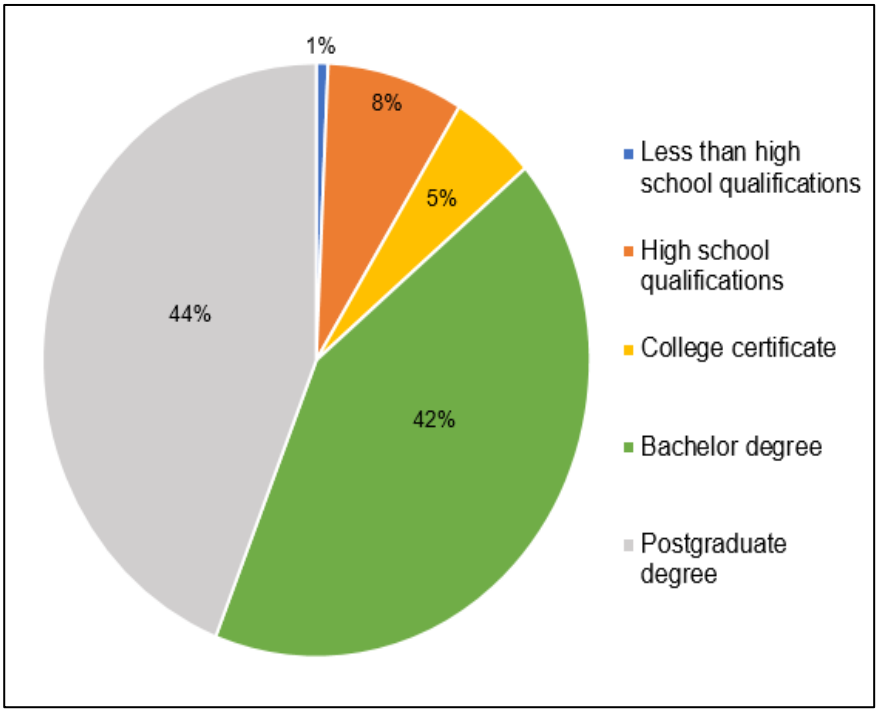


Figure 7.3: Percentages of Participants' Educational Levels

The digital devices skill and technology experience of the participants were assessed using five categories: novice, advanced beginner, competent, proficient and expert. More than a third of the participants (34%) are competent at managing technology. 111 participants (26%) describe themselves as advanced beginners and 71 participants (16%) are novices. While 61 participants (14%) are proficient and 42 participants (10 %) are experts in digital devices as shown in below graph.

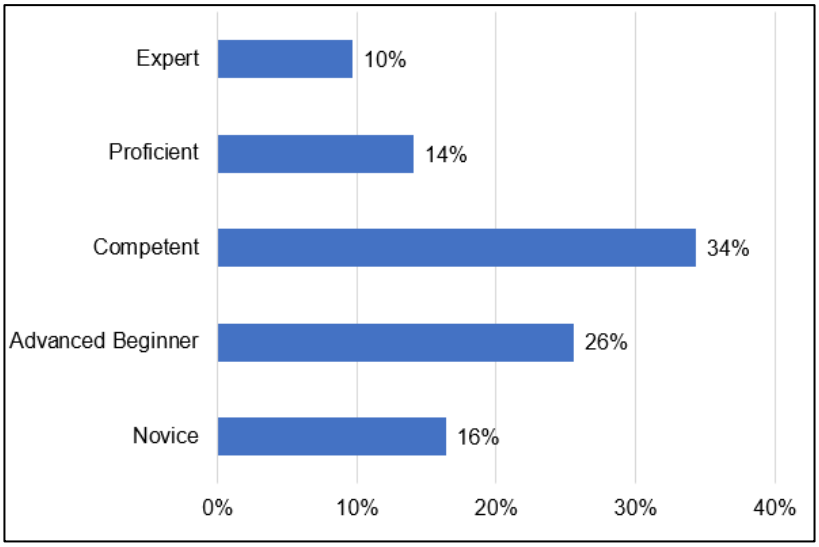


Figure 7.4: Percentages of Participants' Technology Skills

7.3.2 Cyber Security Concerns, Knowledge and Management

7.3.2.1 Cyber Security Concerns

The level of the participants' concerns about different security aspects and controls was assessed in the questionnaire. It was evident that the majority of the participants have a concern about managing and monitoring security and controls in their digital devices. As can be seen from the below graph (see Figure 7.5), around 44% of the participants are extremely or moderately concerned about the security and the safety of their owned digital devices, leading to an arithmetic mean of 3.23. While around 54% feel extremely or moderately concerned about the security and the safety of the digital devices owned by their family members giving an arithmetic mean of 3.50. The results illustrated that more than 40 % of the respondents are moderately or extremely concerned about most of the security settings and controls which can be applied or installed in the digital devices. The arithmetic mean for all the provided elements is above 3.00 except for the concern about parental controls.

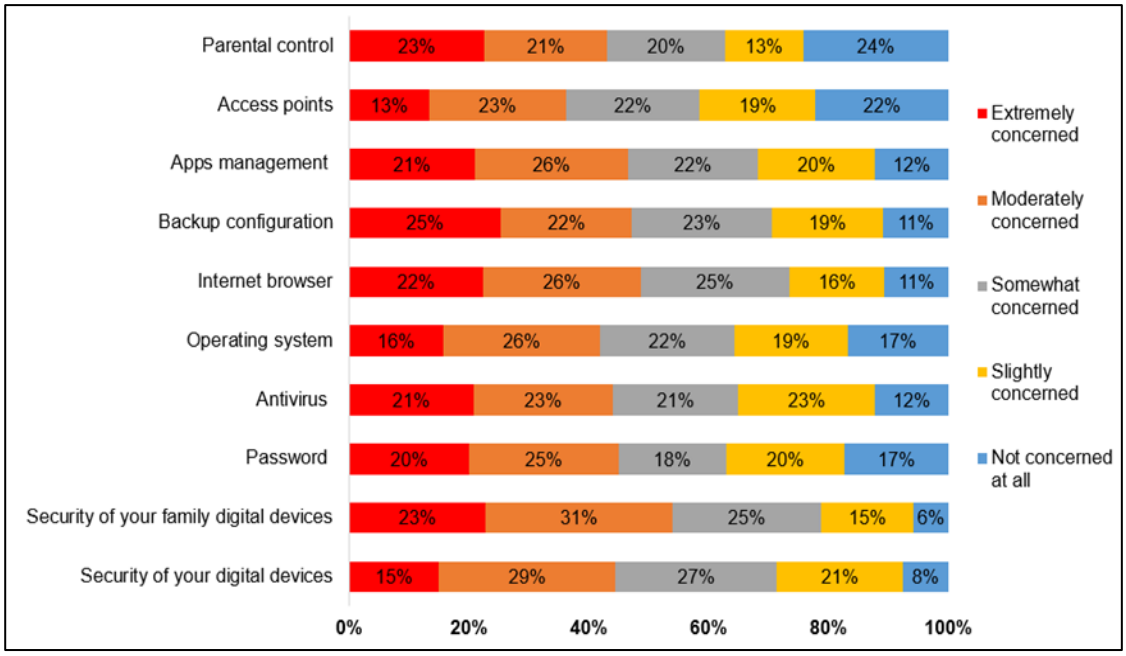


Figure 7.5: Participants' Concerns about Different Security Aspects and Controls

In addition, the result reveals that the participants who described themselves as experts are more concerned than the novice participants in most of the security aspects is shown in Figure 7.5. For example, 43% of the expert participants are extremely concerned about password security and only 5% of them are not concerned at all. 36% of the expert participants said that they have an extreme concern about internet browsing security and fewer than 5% of them have no concern at all. While 28% of the novice participants are extremely concerned about the security of the internet browser and 11% are not concerned at all. This indicates that expert participants are more concerned than other participants who have low technical knowledge and skills because they might understand the importance of these security controls and configurations and the need of implementing and managing these controls.

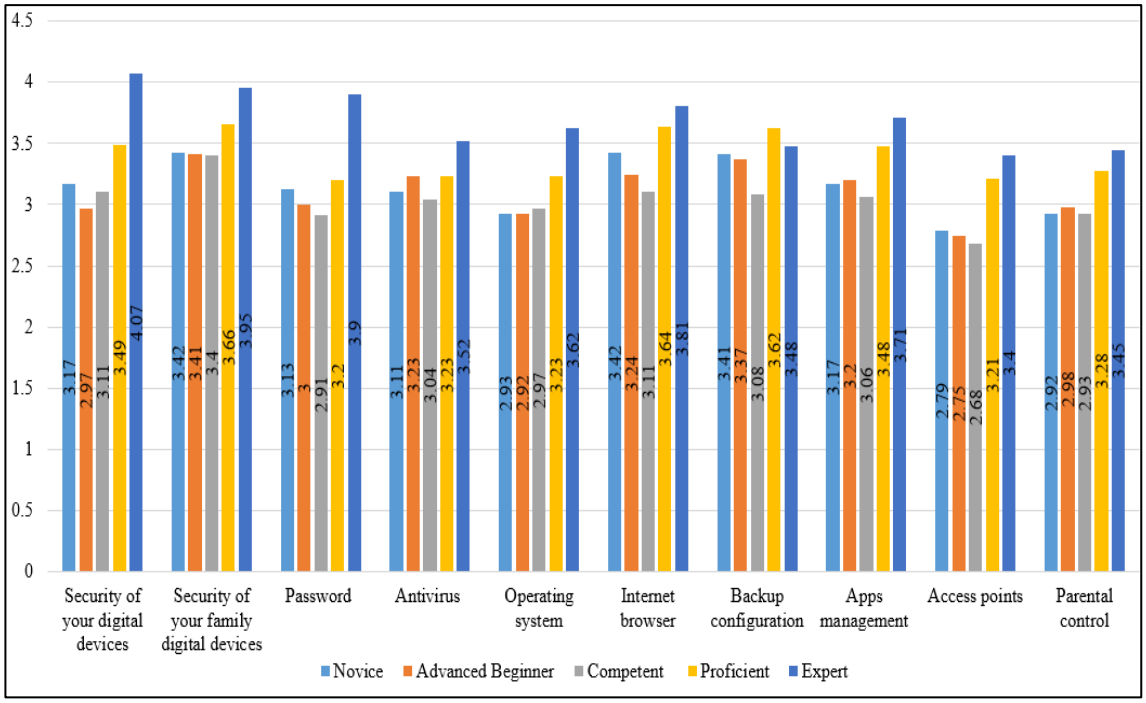


Figure 7.6: Difference in Means between the Participants in Security Concern

The overall insight of the above graphs shows that the respondents are concerned about their digital devices' security including different controls, configurations and services. It was noticed that participants who have more security and technical skills are more concerned about their security as they might realise the potential threats and risk they may face. This can indicate that an effective solution should be developed which can monitor and manage security controls and configurations in digital devices in order to reduce their security concerns.

7.3.2.2 Cyber Security Knowledge

After understanding the users' concerns regarding their digital devices' security, specific questions were asked to assess the participants' knowledge about implementing, managing and monitoring different security aspects and configurations. Figure 7.7 shows more than 40% of the participants stated that they are extremely or moderately knowledgeable about different security aspects such as passwords, antivirus and internet browser security. However, around 30% of the participants have a slight knowledge or

do not have any knowledge about several security aspects such as antivirus, operating system, Internet browser, application management.

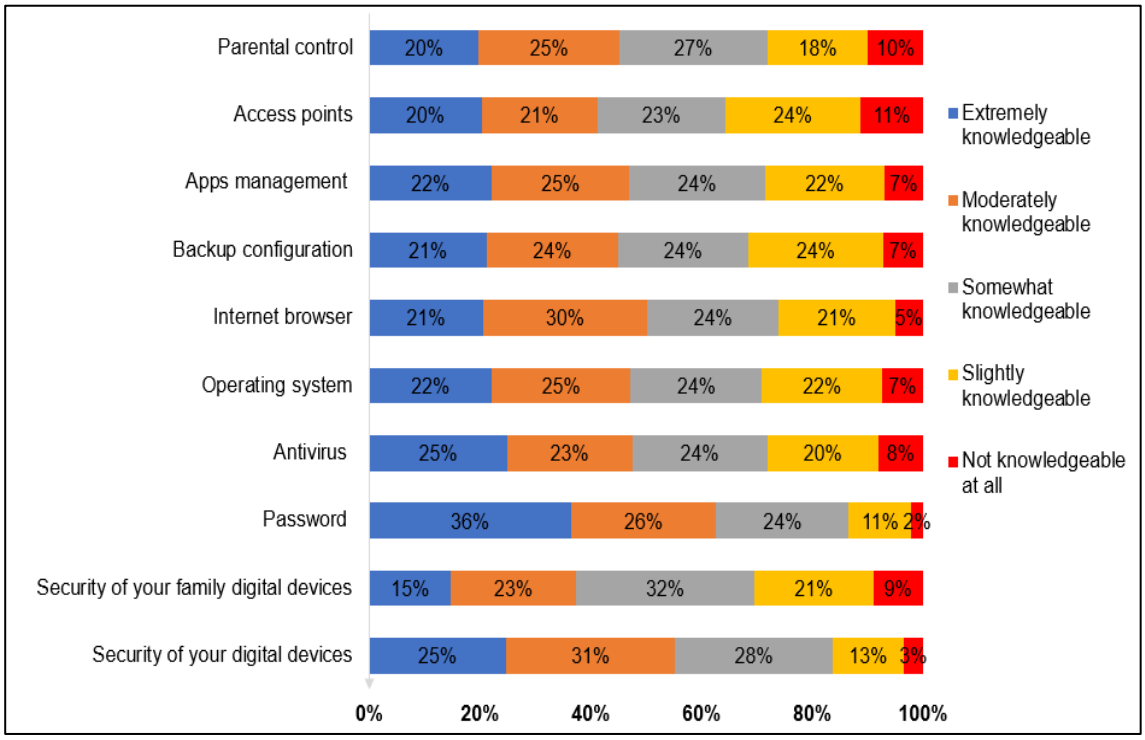


Figure 7.7: Participants' knowledge about Different Security Aspects and Controls

It was shown that participants who have good technical skills have good knowledge of different security aspects and controls as illustrated in Figure 7.8. For example, around 80% of expert participants said that they are extremely or moderately knowledgeable in antivirus protection while 42% of novice users had slight knowledge or no knowledge at all about antivirus. 76% of experts have a moderate knowledge or better on how to keep their operating system secure and protected security while 45% of the novice participants have a slight knowledge or no knowledge at all.

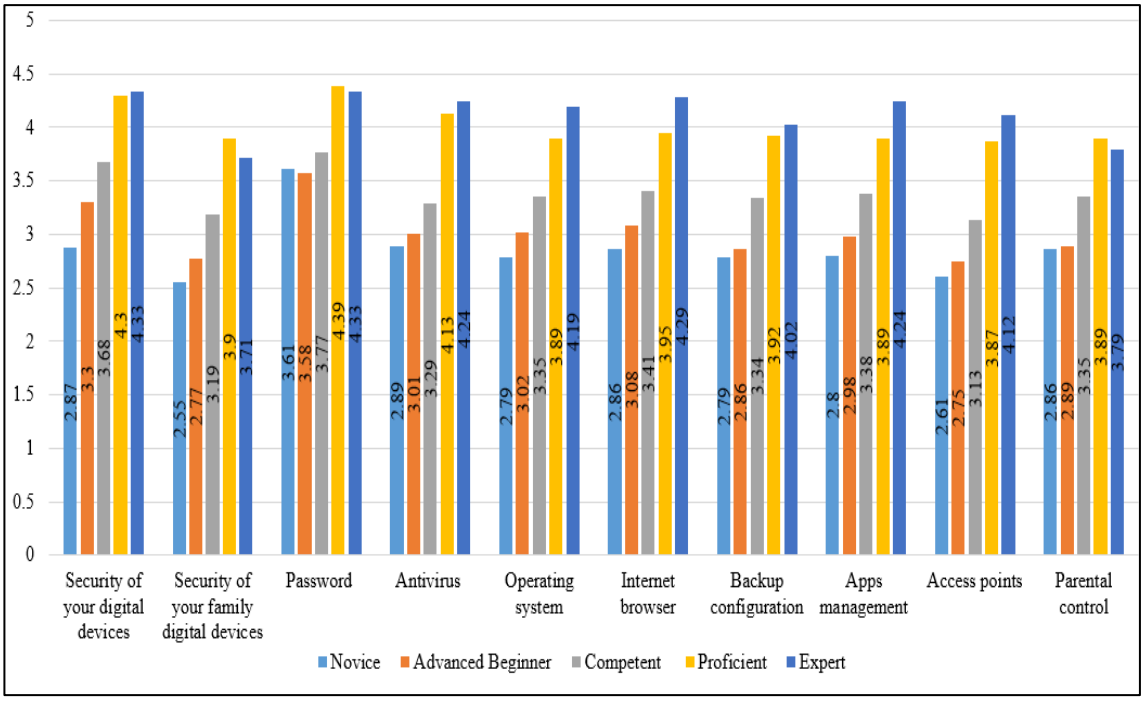


Figure 7.8: Difference in Means between the Participants in Security Knowledge

These results indicate that there is lack of knowledge about some security aspects and practices. This lack increases significantly among the participants who do not have a good level of technical skills. Therefore, an approach can be suggested to provide bespoke information security awareness which can take into consideration the level of the users' security knowledge.

7.3.2.3 Cyber Security Management

Further information was gathered with regard to how participants manage different security settings and controls on their digital devices. As shown in Figure 7.9, around 35% rarely or never try to manage or keep their family members' devices secured. Around 18% rarely or never manage their passwords and 29% rarely or never manage their antivirus respectively. Only 18% claimed that they always manage the security settings of their operating systems while around 30% who rarely or never configure these settings. It was notable that around 30% of the participants rarely or never manage the security settings of their internet browsers and application management. The security

configurations of the access points and parental controls are rarely or never managed by 39% and 34% of the users respectively.

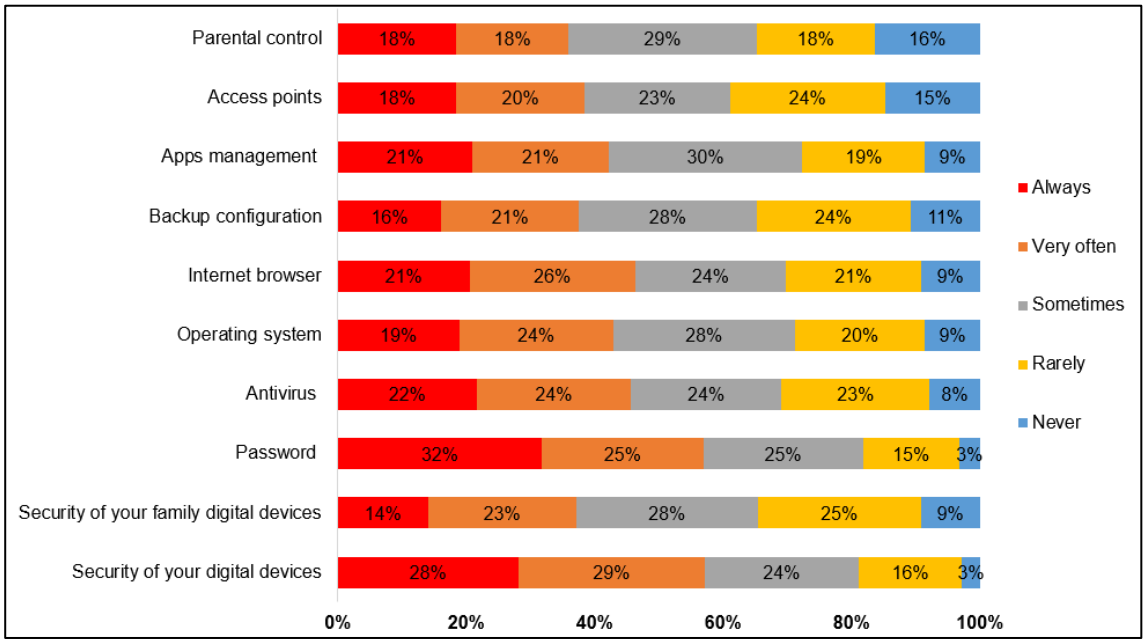


Figure 7.9: Participants' Management for Different Security Aspects and Controls

It was shown that participants who have good technical skills manage their security settings and controls more frequent than other participants who have poor IT skills as shown in Figure 7.10. For instance, operating system security is always or very often managed by 62% of experts while 46% of novices rarely or never managed their operating systems. In addition, 42% of novices rarely or never managed the security of their internet browsers and applications.

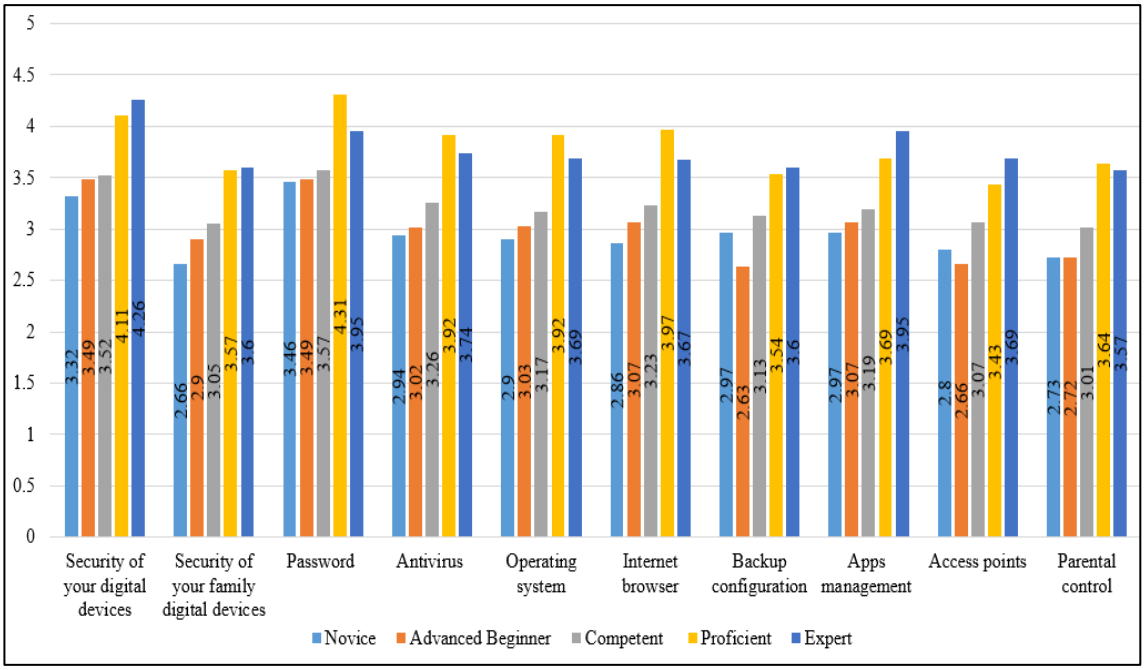


Figure 7.10: Difference in Means between the Participants in Security Management

Overall, the results indicate that some of the security configurations and controls in digital devices. The reason behind this lack of frequent management might be because the participants do not have appropriate security awareness, knowledge or they might not be equipped or not have a strong desire to manage their security regularly. In addition, the results reveal that the lack of security management becomes more noticeable with the participants who do not have a good level of technical experience.

7.3.2.4 Ease of security management

The participants, who stated that they manage their security controls (always, very often, sometimes and rarely), were asked to state how easy is it to manage their security aspects and configurations in order to keep their digital devices protected. As illustrated in Figure 7.11, only 18% of the respondents claimed that it is extremely easy to manage and configure the security settings of their personal devices, 30% find it neither easy nor difficult while 16% claimed that the security management is somewhat difficult as shown. Worryingly, just below 60% who claimed that managing the security settings of the

digital devices belonged to their families is not an easy task or somewhat difficult. 20% experienced a slight or extreme difficulty in managing their antivirus configurations. Around 28% claimed that there is difficulty in managing their operating systems, access points, and application management. 32%, 29% and 28% do not find easy to manage the configurations of parental control, operating systems and internet browsers respectively.

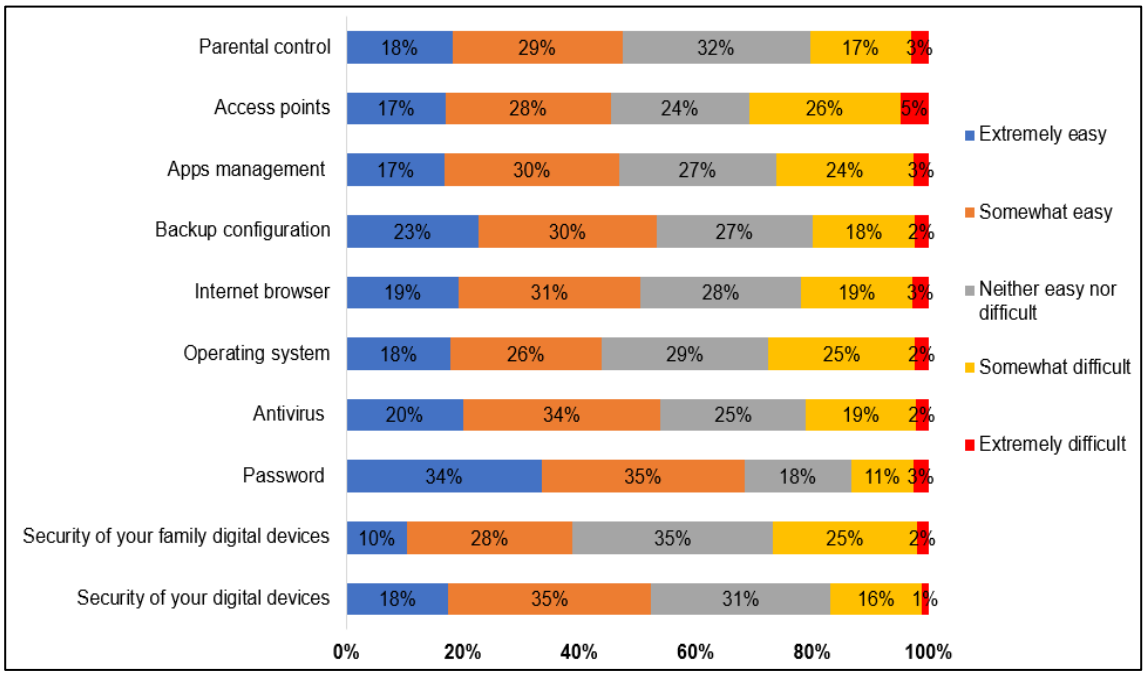


Figure 7.11: Ease of Management Level for Different Security Settings and Controls

Figure 7.12 shows that managing different security controls can be easy for participants who have a good level of technical skills. 73% of the expert participants found the security management of internet browsers is extremely or somewhat easy while 33% of novices found it difficult to be managed and protected. 52% of experts stated that it is an easy task to manage and secure their applications while 27% of novices said it is difficult and 39% found it neither easy nor difficult.

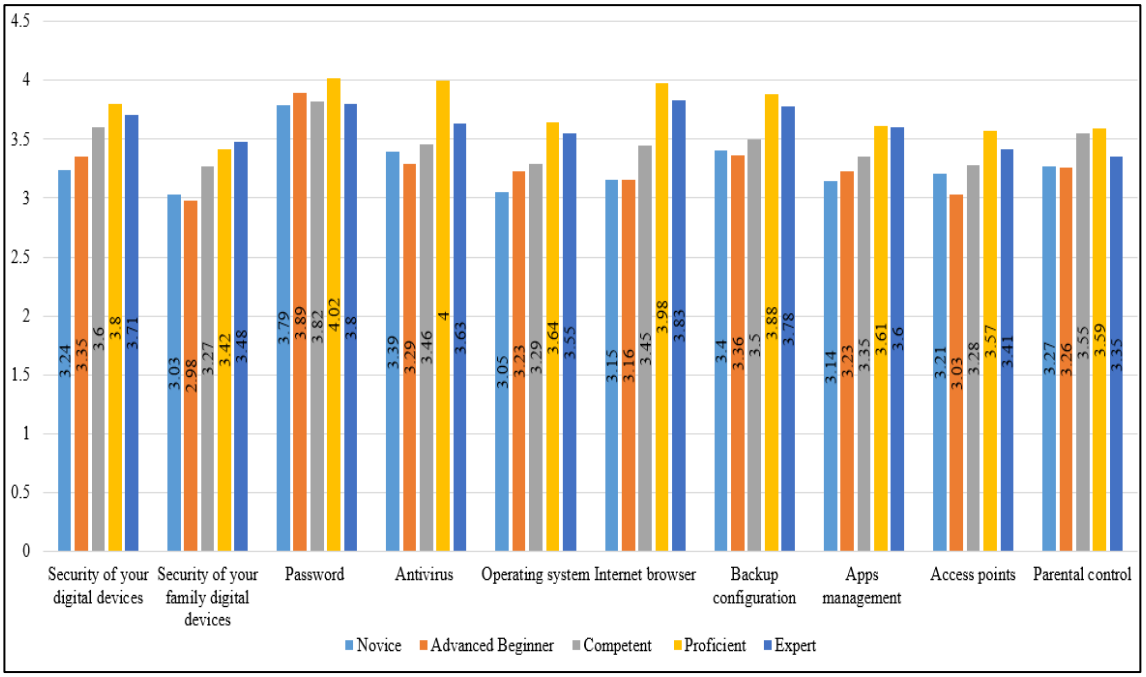


Figure 7.12: Difference in Means between the Participants in Ease of Management

These results suggest that managing different security aspects, controls and configurations in different devices is not an easy task especially for the users who do not have good technical skills. Thus, providing an approach is fundamental which can manage and monitor security controls and configuration in a usable manner based the current needs, prior knowledge, or security priorities for each user, technology and service.

7.3.2.5 Correlation between the Level of Security Concern, Knowledge and Management

Pearson's correlation coefficient test has been conducted to measure the statistical association between two variables as discussed in Chapter 4:

A. Security Concern and Security Management

As shown in Table 7.2, there is a significant positive correlation between the level of security concern and security knowledge in most of the identified security aspects and

controls (6 out of 10 are highly significant (i.e., p-value of 0.01), 3 are significant (i.e., p-value of 0.05) and only 1 is not correlated). This means that when the level of security concern increases or decreases in one of the listed security aspects, the level of knowledge will increase or decrease in the same aspect. For example, the result shows that there is a positive correlation between concern and knowledge about password security. Therefore, if the level of concern about password security increases in users, they will have more knowledge and a desire to learn more about password security and vice versa. Thus, rising security concerns of users by providing them with some facts and statistical information about different security aspects can motivate users to gain more security knowledge about these aspects

Correlation Between Security Knowledge and Security Concern	P value (Sig)	Pearson's correlation	Correlation type
Security and safety for all the digital devices used by you	**0.031**	0.104	Positive
Security and safety for all the digital devices used by your family	**0.033**	0.102	Positive
Password	**0.004**	0.139	Positive
Antivirus	**0.017**	0.115	Positive
Operating system	**0.000**	0.172	Positive
Internet browser	**0.000**	0.225	Positive
Backup configuration	**0.004**	0.137	Positive
Apps management	0.076	0.085	
Access points	**0.000**	0.190	Positive
Parental control	**0.000**	0.275	Positive

Table 7.2: The Correlation between Concern and Knowledge

B. Security Knowledge and Security Management

Another test was conducted to measure the relationship between the level of knowledge and security management. Table 7.3 shows that there is a positive correlation between the

level of knowledge and the level of management in all the security aspects and features among home users. As the level of security knowledge increases in one aspect, users are tended to manage the same security aspect more frequently and better.

Correlation Between Security Knowledge and Security Management	P value (Sig)	Pearson's correlation	Correlation type
Security and safety for all the digital devices used by you	**0.000**	0.550	Positive
Security and safety for all the digital devices used by your family	**0.000**	0.586	Positive
Password	**0.000**	0.525	Positive
Antivirus	**0.000**	0.642	Positive
Operating system	**0.000**	0.637	Positive
Internet browser	**0.000**	0.583	Positive
Backup configuration	**0.000**	0.540	Positive
Apps management	**0.000**	0.588	Positive
Access points	**0.000**	0.648	Positive
Parental control	**0.000**	0.664	Positive

Table 7.3: The Correlation between Knowledge and Management

C. Security Concern and Security Management

As the two above tests show that there is a significant positive correlation between security concern and security knowledge and between security knowledge and security management. Therefore, it can be said that there is also a significant positive correlation between security concern and security management. This means users are tended to manage their security more frequently and better when the level of security concern increases. Thus. An approach needs to be proposed which can improve security management by increasing users' security concern about different security issues and aspects.

D. Security Knowledge and Security Ease of Management

In addition, another test was conducted to measure the relationship between the level of knowledge and how easy to manage different security controls. The result shows that there is a positive correlation between the knowledge and the ease of management in all the identified security aspects as illustrated in Table 7.4. Therefore, if the knowledge of the users increases in different security aspects, the ease of managing these aspects will increase and become easier.

Correlation Between Security Knowledge and Ease of Security Management	P value (Sig)	Pearson's correlation	Correlation type
Security and safety for all the digital devices used by you	**0.000**	0.368	Positive
Security and safety for all the digital devices used by your family	**0.000**	0.207	Positive
Password	**0.000**	0.275	Positive
Antivirus	**0.000**	0.421	Positive
Operating system	**0.000**	0.468	Positive
Internet browser	**0.000**	0.375	Positive
Backup configuration	**0.000**	0.356	Positive
Apps management	**0.000**	0.381	Positive
Access points	**0.000**	0.376	Positive
Parental control	**0.000**	0.292	Positive

Table 7.4: The Correlation between Knowledge and Ease of Management

The above Pearson's correlation tests reveal that there is a positive correlation between the security concern, knowledge and management toward different security aspects and controls. Therefore, an approach can be suggested that can increase and promote security concerns and knowledge in different security subjects and aspects in order to have better

security management. By achieving better and frequent management for different security aspects, users will find it easier to manage different security controls and aspects as evident by the above results.

7.3.3 The Impact of Age, Technical Skills and Education on Security Concern, Knowledge, Management

As discussed in Chapter 4, Pearson's correlation coefficient test has been conducted to measure the association between the age group, technical skills and education on the level of concern, knowledge management and ease of management for different security aspects and features. In addition, Oneway ANOVA test was also conducted to determine whether there is any statistically significant difference between means of different variables in different scales.

Investigating the impact of age, technical skills and education on security awareness can help to understand the security behaviour of the respondents. In addition, it can facilitate the process of selecting the appropriate security profile for the users in the proposed framework.

7.3.3.1 Age Association with Security Concern, Knowledge and Management

The result shows that there is no significant correlation between the age factor and the level of concern, knowledge and management in most of the identified security aspects as shown in Table 7.5. However, it is found that there is a positive correlation between the age group and the level of concern for the security of the operating system, application and software, access points and parental controls. This lack of correlation might be because there are two groups (55-64 and 65 or older) only have 1 participant for each group and 77% of the participants are from two groups 25 – 34 and 35 – 45. In addition, the age of the participants is ranged in 6 age groups from 18 until 65 and older without

including the children group which is highly likely to have lack of concern, knowledge and management for their devices' security which might make potential risks and threats.

Interestingly, the findings show that there is a negative relationship between the age factor and the ease of managing some security features and controls. It indicates that when the user's age increases, the ease of security management might decrease and become difficult. It means that managing different security features and controls in different devices and technologies might be more difficult for old people.

	Concerns		**knowledge**		**Management**		**Ease of Management**	
	P value	**Correlation**	**P value**	**Correlation**	**P value**	**Correlation**	**P value**	**Correlation**
Security of your digital devices	.052	.093	.827	-.011	.802	.012	**.008**	-.130
Security of your family digital devices	.546	.029	**.004**	.139	**.000**	.168	.099	.083
Password	.160	.068	.465	-.035	.181	-.064	**.023**	-.111
Antivirus	.066	.088	.093	.081	.144	.070	.656	-.022
Operating system	**.005**	.135	.717	.017	.328	.047	.229	-.060
Internet browser	.457	.036	.980	.001	.906	.006	**.045**	-.101
Backup configuration	.182	.064	.600	-.025	.828	.010	**.002**	-.158
Apps management	**.044**	.097	.247	.056	.312	-.049	**.048**	-.099
Access points	**.039**	.099	**.011**	.122	.150	.069	.133	-.078
Parental control	**.000**	.230	.079	.084	**.001**	.165	.463	-.039

Table 7.5: Age Association with Security Concerns, Knowledge, Management

Oneway ANOVA test was also conducted to determine whether there is any statistically significant difference between the different age groups. Table 7.6 shows that there is no significant difference in the level of concern, knowledge and management in most of the identified aspects. However, the result indicates that there is a significant difference between the different age groups in the ease of managing the security of internet browser, backup configuration and the software and application management and the security of their devices in general.

	Concerns		knowledge		Management		Ease of Management	
	F	P Value	F	P Value	F	P Value	F	P Value
Security of your digital devices	1.121	.348	0.792	.556	0.465	.802	2.861	**.015**
Security of your family digital devices	0.548	.740	2.928	**.013**	3.199	**.008**	1.431	.212
Password	0.779	.565	0.642	.668	0.905	.477	1.726	.127
Antivirus	1.323	.535	1.881	.096	0.787	.559	0.725	.605
Operating system	2.127	.061	0.435	.824	0.545	.742	1.842	.104
Internet browser	0.463	.804	0.554	.735	0.463	.804	2.3	**.044**
Backup configuration	0.752	.585	1.047	.389	0.602	.698	3.299	**.006**
Apps management	1.451	.205	1.019	.406	0.971	.435	2.575	**.026**
Access points	1.598	.159	1.981	.081	1.14	.338	1.641	.148
Parental control	5.004	**.000**	1.329	.251	3.833	**.002**	1.157	.331

Table 7.6: The Result of Oneway ANOVA Test for The Age Groups

7.3.3.2 Technical skills Association with Security Concern, Knowledge and Management

The result of Pearson's correlation coefficient test shows that there is a positive correlation between the IT experience level and the level of concern, knowledge and management in most of the identified security aspects as shown in Table 7.7. It means that if a user has a good level of technology experience, he tends to have a better level of concern, knowledge, management and easier management in most of the security features and configurations.

IT experience	Concerns		knowledge		Management		Ease of Management	
	P value	Correlation	P value	Correlation	P value	Correlation	P value	Correlation
Security of your digital devices	**.000**	.210	**.000**	.432	**.000**	.248	**.000**	.182
Security of your family digital devices	.17	.114	**.000**	.367	**.000**	.251	**.001**	.171
Password	**.016**	.115	**.000**	.245	**.000**	.191	.674	.021
Antivirus	.281	.052	**.000**	.351	**.000**	.243	**.003**	.150
Operating system	**.005**	.134	**.000**	.345	**.000**	.244	**.002**	.154
Internet browser	.070	.087	**.000**	.368	**.000**	.245	**.000**	.251
Backup configuration	.669	.021	**.000**	.343	**.000**	.217	**.004**	.144
Apps management	**.033**	.102	**.000**	.358	**.000**	.235	**.004**	.144
Access points	**.006**	.131	**.000**	.372	**.000**	.227	**.033**	.111
Parental control	**.043**	.097	**.000**	.286	**.000**	.237	.156	.075

Table 7.7: Technical skills Association with Security Concerns, Knowledge, Management

In addition, the result of Oneway ANOVA test shows that there is a statistically significant difference between the different levels of technology experience in the level of concern, knowledge and management for almost all the identified security features and configurations as shown in Table 7.8.

	Concerns		knowledge		Management		Ease of Management	
	F	P Value	F	P Value	F	P Value	F	P Value
Security of your digital devices	8.579	**.000**	25.785	**.000**	8.692	**.000**	4.14	**.003**
Security of your family digital devices	2.362	.053	19.031	**.000**	7.935	**.000**	3.472	**.008**
Password	4.56	**.001**	9.087	**.000**	7.161	**.000**	0.491	.743
Antivirus	1.239	.294	17.651	**.000**	8.382	**.000**	4.686	**.001**
Operating system	2.811	**.025**	14.919	**.000**	9.157	**.000**	2.828	**.025**
Internet browser	3.754	**.005**	17.485	**.000**	8.946	**.000**	8.185	**.000**
Backup configuration	2.309	.057	15.58	**.000**	8.344	**.000**	2.86	**.023**
Apps management	2.671	**.032**	16.354	**.000**	7.296	**.000**	2.281	.06
Access points	3.76	**.005**	18.856	**.000**	7.033	**.000**	2.089	.082
Parental control	1.569	.182	11.077	**.000**	7.873	**.000**	1.627	0.167

Table 7.8: Oneway ANOVA Test for Technical skill Levels

7.3.3.3 Education Association with Security Concern, Knowledge and Management

Table 7.9 shows that the result of Pearson's correlation coefficient test illustrates that there is no correlation between the level of education and the level of concern, knowledge, management and the ease of management in most of the security aspects and controls.

Educational level	Concern		knowledge		Management		Ease of Management	
	P value	Correlation	P value	Correlation	P value	Correlation	P value	Correlation
Security of your digital devices	**.042**	.098	.412	-.040	.881	-.007	.151	-.070
Security of your family digital devices	.388	.042	**.010**	.124	.194	.062	.358	-.046
Password	.146	.070	.859	.009	.402	-.040	.153	-.070
Antivirus	.316	.048	**.012**	.120	.350	.045	.651	.023
Operating system	.171	.066	.944	-.003	.830	-.010	.191	-.066
Internet browser	.376	.043	.777	.014	.923	.005	.202	-.064
Backup configuration	.250	.055	.746	-.016	.559	.028	**.023**	-.116
Apps management	.428	.038	.515	-.031	**.043**	-.097	.149	-.073
Access points	.300	.050	.243	.056	.847	-.009	**.004**	-.149
Parental control	.144	.070	.078	.085	.164	.067	.089	-.089

Table 7.9: Education Association with Security Concerns, Knowledge, Management

In addition, Table 7.10 illustrates the result of Oneway ANOVA test which shows that there is no a statistically significant difference between the different levels of education in the level of concern, knowledge and management for most of the security features and configurations except the level of concern towards password, antivirus, operating system settings and the parental controls. This might because the vast majority of the participants (86%) have bachelor or postgraduate degree and only 14% who have less degrees. In addition, the correlation test has shown that there is no type of relationship between the level of the education and the level of concern, knowledge and management of several security controls.

	Concern		knowledge		Management		Ease of Management	
	F	P Value	F	P Value	F	P Value	F	P Value
Security of your digital devices	2.179	.073	.862	.487	.532	.712	1.724	.144
Security of your family digital devices	0.358	.838	2.862	**.023**	.583	.675	.449	.773
Password	2.365	.052	1.142	.336	1.585	.177	1.935	.104
Antivirus	2.644	**.033**	2.055	.086	.765	.548	3.159	**.014**
Operating system	3.4	**.009**	1.07	.371	.795	.529	0.792	.531
Internet browser	1.108	.352	.775	.542	.752	.557	0.882	.474
Backup configuration	1.179	.319	1.499	.201	1.865	.116	3.386	**.01**
Apps management	1.131	.341	.934	.444	1.667	.157	1.132	.341
Access points	1.715	.146	1.221	.301	.599	.664	2.851	.024
Parental control	2.534	**.041**	1.46	.213	1.571	.181	1.634	.165

Table 7.10: Oneway ANOVA Test for Educational Levels

The above different tests have been conducted to measure the association of age, education and technical skills with security concern, knowledge and management. The results indicate that there is a significant positive association between the level of technical skills and the level of security concern, knowledge and management. Therefore, it can be suggested that security management, knowledge and awareness cab offered with different content and approaches to end-users based on their level of technical skills.

7.3.4 Security Concepts for The Proposed Approach

Figure 7.13 reveals an interesting result where the participants expressed a great agreement ((82% strongly or somewhat agreed, leading to an arithmetic mean of 4.24)

with the idea of applying different levels of security settings and controls such as low, medium and high. These different levels can be applied and focused upon the user which was strongly and somewhat agreed by 35% and 30% of the users respectively (leading to an arithmetic mean of 3.84). 37% strongly agreed with the statement that one security level should be applied to all the digital devices owned by one user while 26% somewhat agreed with this statement. In contrast, only 17% and 5% disagreed with the previous suggestion (arithmetic mean of 3.73). 74% of the users strongly or somewhat agreed with providing pre-defined templates of security settings. In contrast, only 8% strongly or slightly disagreed with the pre-defined templates (leading to an arithmetic mean of 4.00).

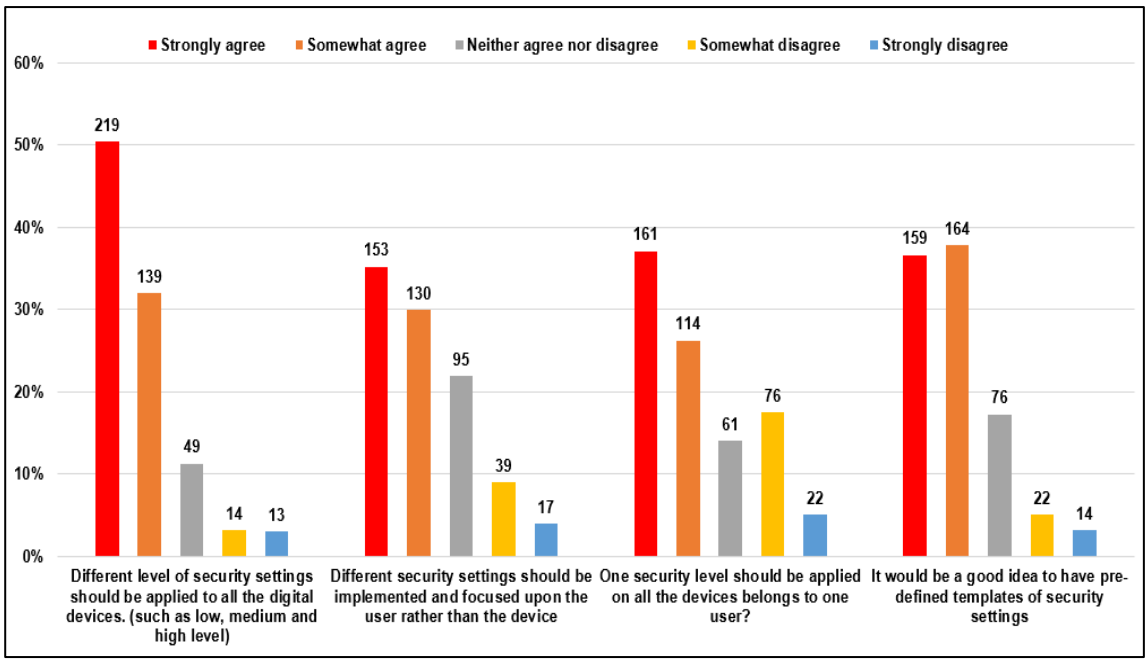


Figure 7.13: The Agreement of the Participants towards Some Security Concepts

These concepts might require a good level of technical experience and knowledge and might be difficult for novice users to discuss and make an appropriate decision to improve information security. The responses of the participants who described themselves as experts and proficient are reviewed regarding the above security concept. The result, after excluding the participants who do not have good security experience, reveals that there is no major change in the level of the agreement with the above security concepts.

7.3.5 End-users' Feedback about The Proposed Interfaces

As discussed in Chapter 4, a questionnaire is conducted to get feedback on the preliminary interface designs for the proposed framework, which are introduced in the previous chapter (Chapter 6). Two interface designs were developed for each component in the proposed approach. The participants were asked to assess the following aspects of each design:

- Structure
- Icons
- Understanding the interface purpose
- Colours
- Coherence
- Ease of use
- Texts
- Sections' sequence
- Information relevance

The following subsections discuss the feedback received from the participant on the two proposed interface designs for each component.

7.3.5.1 Main Dashboard

As can be seen in Figure 7.14, satisfactory feedback received from the participants on the two proposed designs for the main dashboard. Only fewer than 6% of the participants found the aspects of the two proposed designs poor. While the vast majority of the respondents stated that the structure, colours, text and icons, ease of use and information relevance are good or better.

The participants were asked to choose which interface they would prefer to use. 52% of the respondents chose the first proposed interface while 48% were with the second interface. Therefore, the first proposed design of the dashboard will be used as a main dashboard interface in the final proposed design.

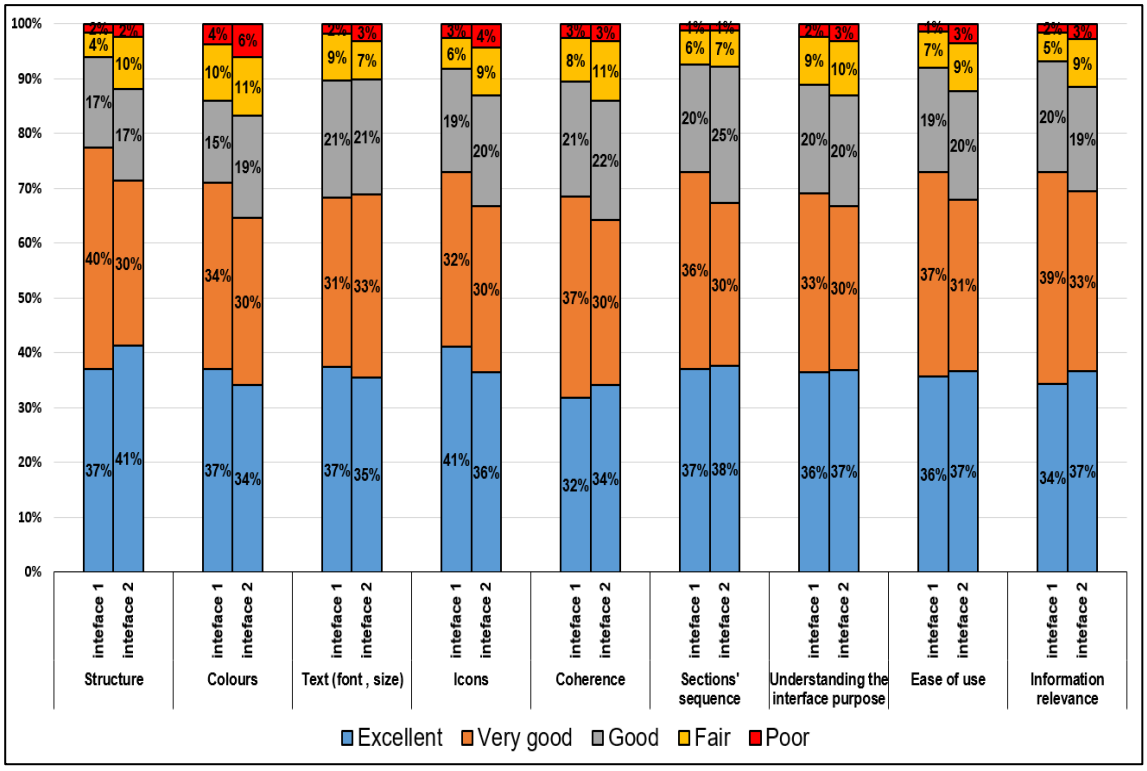


Figure 7.14: End-Uers' Thoughts about The Two Designs for Dashboard

7.3.5.2 Enrolment Interface

Overall, more than 74% of the respondents assessed the aspects in the two proposed designs for the enrolment interface such as structure, colours, icons, ease of use and coherence with excellent or very good while fewer than 3% said that these aspects were poor as illustrated in Figure 7.15. This indicates the two designs including their aspects and elements are highly accepted by the participants.

The participants were also asked to select which interface they would like to use in the proposed system. 60% of the respondents stated that they prefer the second proposed interface (Point-and-Click approach) while 41% preferred to use the second proposed interface (Drag-and-Drop approach). Therefore, the first proposed interface will be used in the final design as main interface which can handle any enrolment processes.

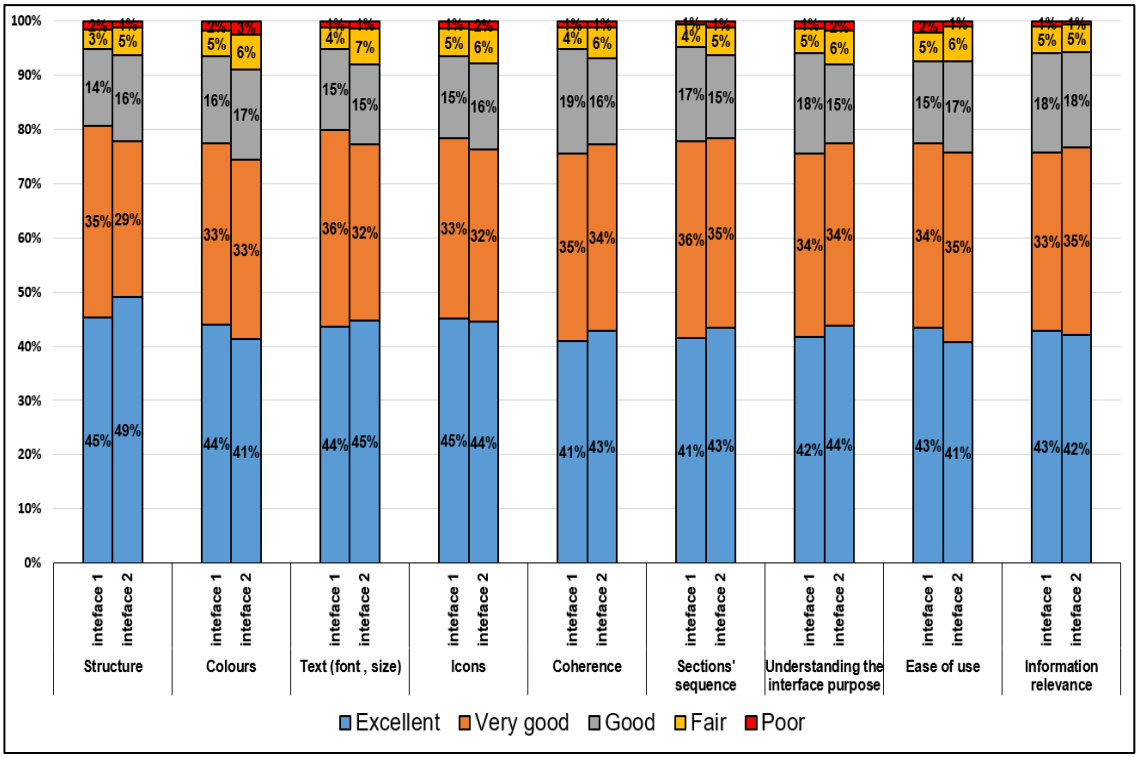


Figure 7.15: End-Uers' Thoughts about The Two Designs for Enrolment

7.3.5.3 Management Interface

As demonstrated in Figure 7.16, fewer than 3% of the respondents stated that the structure, icons, colours, texts, coherence and the other aspects are found poor while the majority are satisfied with all the components and aspects in the two interface designs. However, the aspects and elements of the second interface were found better than the first interface. For example, 60% of the participants stated that the structure of the second interface is excellent while 37% found it excellent in the first design excellent or very good. The participants were asked to select which interface they prefer to use. Most of them (79%) preferred using the second proposed interface (hierarchical style) while 21% chose the first proposed interface (Red and Green).

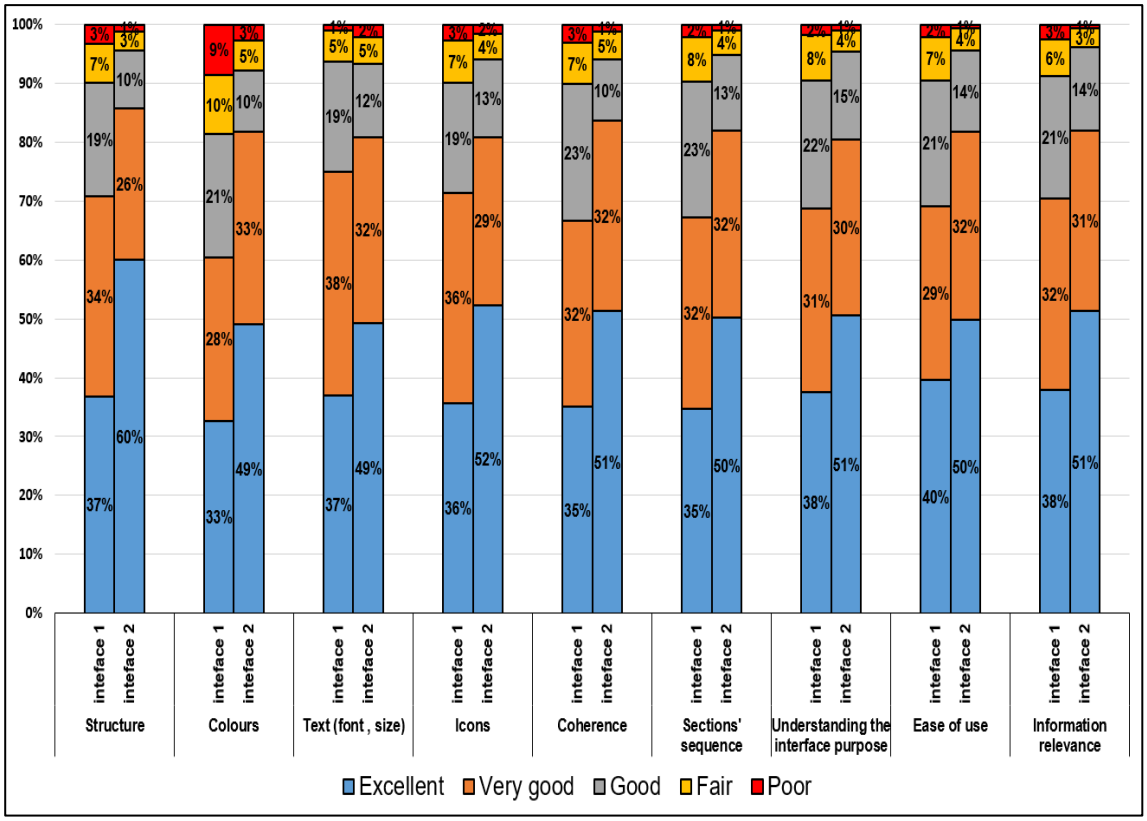


Figure 7.16: End-Uers' Thoughts about The Two Designs for Management

7.3.5.4 User Profile Interface (For Administrators)

The presented results in Figure 7.17 show an excellent level of satisfaction about the elements and the components of the two proposed designs. Fewer than 3% stated the two interfaces are poor while around 90% found the components and elements of the two designs good or better.

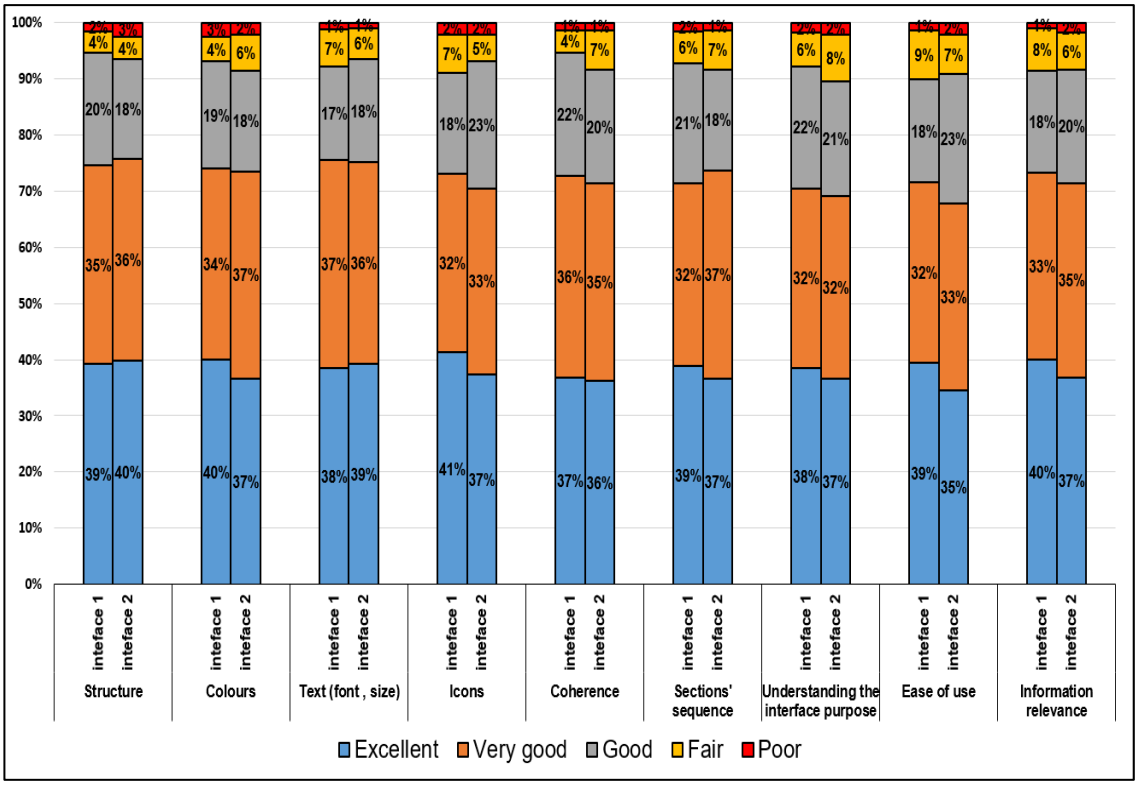


Figure 7.17: End-Uers' Thoughts about The Two Designs for User Profile

Although there is no major difference in the feedback between the two proposed designs, the respondents were asked to choose the interface design which they would like to use, 53% preferred the first proposed interface (horizontal menu) while 47% chose the first interface (clickable boxes).

7.3.5.5 End-Users Profile

Figure 7.18 demonstrates that the participants provide satisfactory feedback on the two proposed interfaces for end-user's profile. The elements and the aspects of the two interfaces are found poor by fewer than 3%. The second interface is found slightly better than the first interface in most of the components and elements such as structure, colours and ease of use. More than half of the respondents (56%) preferred the second proposed interface (expandable/collapsible Sections) while 44% selected the first proposed

interface (clickable boxes). Therefore, the first interface will be used in the final design to visualise end-user's profile

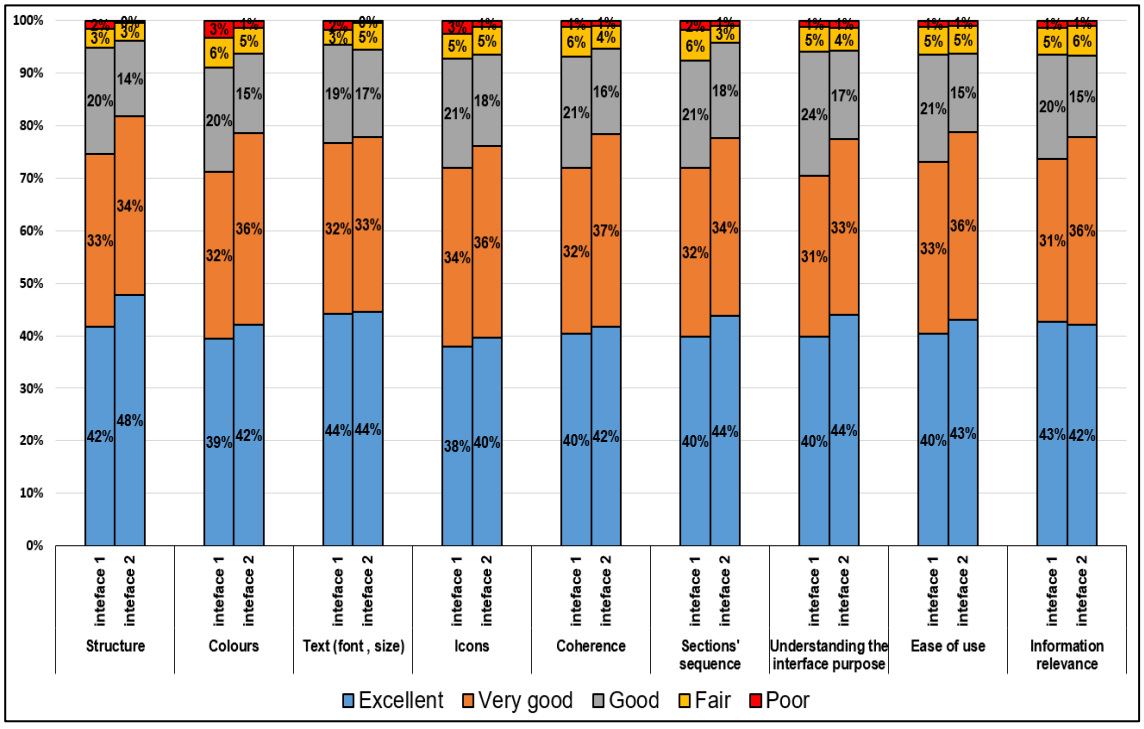


Figure 7.18: End-Uers' Thoughts about The Two Designs for End User Profile

As the usability aspects might require a good level of technical experience and knowledge and might be difficult for novice users to discuss and provide appropriate feedback about the different designs. The feedback of the participants who described themselves as expert and proficient are reviewed regarding the above proposed interfaces. The result, after excluding the participants who do not have good security experience, reveals that there is no major change in the received feedback for the above interface designs.

7.3.5.6 Comments analysis

Several interface designs have received many interesting comments. A few comments were regarding the colours used in the interfaces, suggesting red and green should be lighter in order to make eyes comforted. In addition, it was suggested that the background colour should be changed from grey to a better colour such as blue. One of the identified

interesting comments was that the designed profile only shows one device for each user what about if the user has more than one device, suggesting that the profile should include all the devices owned by one user and make it easy to move between the devices. A number of participants, who claimed that they have a good level of technical experience, suggested that it is a good idea if the solution can provide users with educational material and encourage them to learn more in a motivational way. Other comments suggested that the main dashboard should be configured easily based on the needs of the administrators. The overall comments analysis that the majority of the participants were satisfied with the proposed design, however some aspects were suggested to be improved.

7.4 Discussion

The results of the survey are collected from 434 participants with a verity of backgrounds in terms of gender, age, educational level and technology experience. The results reveal that the respondents are concerned about the security practices and controls which have been applied to their digital devices and their family members' devices. It was evident that the participants, who have better technical skills, are more concerned about their devices' security because they have enough skills which can enable them to understand and realise the importance of their devices' security and the potential threats which might happen by implementing weak security.

It is also perceived that more than half of the participants are somewhat knowledgeable or less about how to implement and manage security practices and security controls on their digital devices. The results show that the participants with good technical skills have better knowledge in managing security controls and configuration in their devices. Although around 60% of the participants state that they have good technical skills and only 10% and fewer do not have any security knowledge, The findings show that more

than half of the participants they sometimes or never manage or monitor their devices' security. The reason behind this unsatisfactory security management is that the participants might be busy or not prepared very well to manage and monitor information security in different devices. Another reason is that users might find it difficult to manage their security as it is evident from the findings that more than half of the participants stated that it is not an easy task to implement and manage their security controls on their digital devices.

It is also perceived that there is a significant association between the technical skills and the level of cyber security concern, knowledge and management for different security configurations and controls. As a result, the level of concern, knowledge and management would vary across different levels of technical skills as it is shown in the results that the users who have good IT skills usually have more knowledge and manage their digital devices more frequently than others who have a low experience level. The participants with low technology experience (Novice and advanced beginners) are found to have less concern, less knowledge, rare management and more difficulty in managing, controlling and configuring all the security controls and configurations. As a result, they can experience more cyberattack easily and make the home network and connected devices more vulnerable to online threats.

In addition, the results demonstrate a positive association between the level security concern, the level of security knowledge and the management frequency for different security controls and aspects. It means that when the level of security concern is increased, the security knowledge can be improved and the security management can be enhanced. Therefore, it can be suggested that an approach needs to be proposed which have the ability to increase the level of security concern in order to increase and improve

security knowledge for users. Once these two elements get improved, users can manage their security more frequent and easier as illustrated in the findings.

As presented in the previous section, the findings reveal that the main concepts for the proposed approach are agreed by the majority of the respondents. A high percentage with 82% of the respondents strongly or somewhat agreed that different levels of security settings such as low, medium and high should be applied to all the digital devices. In addition, providing pre-defined templates of security settings is agreed by around three quarters of the respondents. The idea that the different levels should be focused on the users, not the device is strongly and somewhat agreed by 35% and 30% respectively. Another suggestion is that one security level can be applied to all the digital devices owned by one user is strongly or somewhat agreed by 63% of the respondents. All these concepts and ideas would be used in the final solution and framework in the next chapter.

In general, very good thoughts and feedback were received by the majority of the participants for all the proposed interface designs. The designs were assessed in terms of different usability elements such as the structure, colours, texts, icons coherence, ease of use and information relevance. The percentage of the participants who claimed that some elements were poor did not exceed 4% except 8% who stated that the colours were poor for only one interface design. The most preferred design interface of the two designs for each component will be used as main interface for each component in the proposed framework.

Several comments have been received from the participants for each interface design and discussed in the previous section. It is suggested that the current proposed interface design for user profile can be enhanced and improved to include all the digital devices owned by one user. Therefore, it would be a good idea if the tool has the ability to provide the users

with a comprehensive profile in a usable method which includes all the devices belongs to each user which can allow the user to monitor and move between the devices easily. Some suggestions were about the colours used in the interface especially the degree of the red colour which needs to be improved and enhanced in order to make the interface appearance comfortable and attractive.

7.5 Summary

The survey findings show that there is a strong positive correlation between the level of technology experience and the level of security concern, knowledge and the frequency level the security management for different security aspects and controls. In addition, the results demonstrate that there is a positive association between the level of security concern and security knowledge, and management frequency in terms of different security aspects and configurations. A satisfactory agreement received from the participants about the idea of applying different levels of security policies for providing better security management. In addition, the majority of the participants agreed that the idea of providing users with pre-defined templates would help users and enhance their security management. The feedback received from the participants about the initial interfaces in terms of different usability and functionality aspects was very satisfactory with high percentage. However, some suggestions have been made by the respondents which might help in improving the final solution. Considering these results and feedback, the next chapter presents the system architecture, mock-up design and focus groups results.

Chapter Eight

System Architecture and Evaluation

8 System Architecture and Evaluation

8.1 Introduction

With aforementioned feedback and results about the information security concern, knowledge and management for home users towards different security aspects and features (described in the previous chapters). In addition, after discussing the feedback on the proposed initial interfaces in the previous chapter. Therefore, these results are used to propose a framework which aims at improving the information security management and awareness for home users. The framework is intended to provide better security management and awareness for home users by applying different groups of security policies in order to measure and monitor several security aspects including settings, configurations and controls.

In this chapter, a comprehensive description of the system architecture requirements, components and processes is explained showing the flexibility of managing different security aspects for different devices and operating systems. Moreover, a mockup design with interactions is designed in order to prove the concept of the proposed solution and how it can work in a real environment. This chapter provides the results of the two focus group sessions, that were discussed in detail in Chapter 4, which were conducted to evaluate the proposed approach.

8.2 System Requirements

There are several initial system requirements which were identified, presented and discussed in Chapter 5, which need to be considered in the proposed approach. However, these requirements are reviewed and improved based on the feedback received from the participatory study (questionnaire). The following requirements need to be considered and addressed in the proposed architecture:

- **Security policies:** different groups of security policies are required to be defined and assigned for devices and users. The policies should cover different operating systems and technologies including their security configurations and controls which can enhance their protection and security once being configured and managed effectively.
- **Security levels:** the security policies can be configured and defined based on three levels: low, medium and high. This can provide good flexibility and granularity in the proposed system in order to meet the users' needs. For instance, the low level can contain the minimum requirements which need to be configured in the devices and it can be assigned for novice users who do not have good technology experience.
- **Usable interfaces:** the components of the system interfaces should be easy to access, use and understand in order to help the system to achieve its main objectives and goals. The interfaces need to be designed based on HCI and usability principles in order to meet the users' requirements and satisfaction.
- **Automatic recognition sensor:** the system should have an automatic recognition feature which can allow it to scan, identify and recognise new digital devices which have not been enrolled in the system yet in order to be added. The system should have the ability to assign an appropriate security policy for the recognised device.
- **Automatic security check:** the proposed system should review continuously the configured security settings and controls on the managed devices in order to be compared with the assigned policies in order to check the security compliance.
- **The selection of security level and user profile:** as the results show that the level of technical skills and experience have an impact on the security concern, knowledge and management. Therefore, the security level and profile should be selected based on the user's skills and knowledge.

- **The enrolment process:** the system should be able to provide different enrolment process for different types of users: novice, intermediate and advances. For example, the novice users should be given an almost automatic configuration process where is a little to nothing for them to have to do, including baseline security measure is used to provide A level of protection for them.
- **Security Concern and Knowledge:** the system should have the ability to raise security concerns and knowledge in order to raise and improve security management as it is evident by the results of the questionnaire.
- **A tailored security awareness content:** the proposed system should be able to deliver tailored security awareness customised based on the users' knowledge and their current needs. This will help to deal effectively with different types of users who have different levels of knowledge and requirements.
- **A Flexible design:** the system should have a level of flexibility by providing a settings page that allows the users (administrator and end-user) to change interface themes, colours and the dashboard sections.
- **A comprehensive profile:** The system should have the ability to provide the users (administrator and end-user) with a comprehensive profile in a usable method which includes all the devices belongs to each user which can allow the user to monitor and move between the devices easily.
- **A competitive educational environment:** the system should have the ability to encourage the family members to do better security and gain more knowledge by providing several methods such as quizzes and digital badges and scores.

All the above system requirements have been achieved and by utilising the information security management architecture which is described in the next section.

8.3 The Architecture

Stemming from the abovementioned requirements, cyber security management and awareness framework is proposed. The proposed system built upon this framework would provide a user-friendly approach based on the user's current needs including a bespoke security awareness that can help in providing better security management and awareness.

In this framework, the administrator is able to monitor and manage different security settings and control in different digital devices within the home environment. In addition, it allows the end-users to check their security compliance with their assigned policies and make them aware of any potential threats or issues. Figure 8.1 demonstrates the overall architecture of the cyber security management and awareness system.

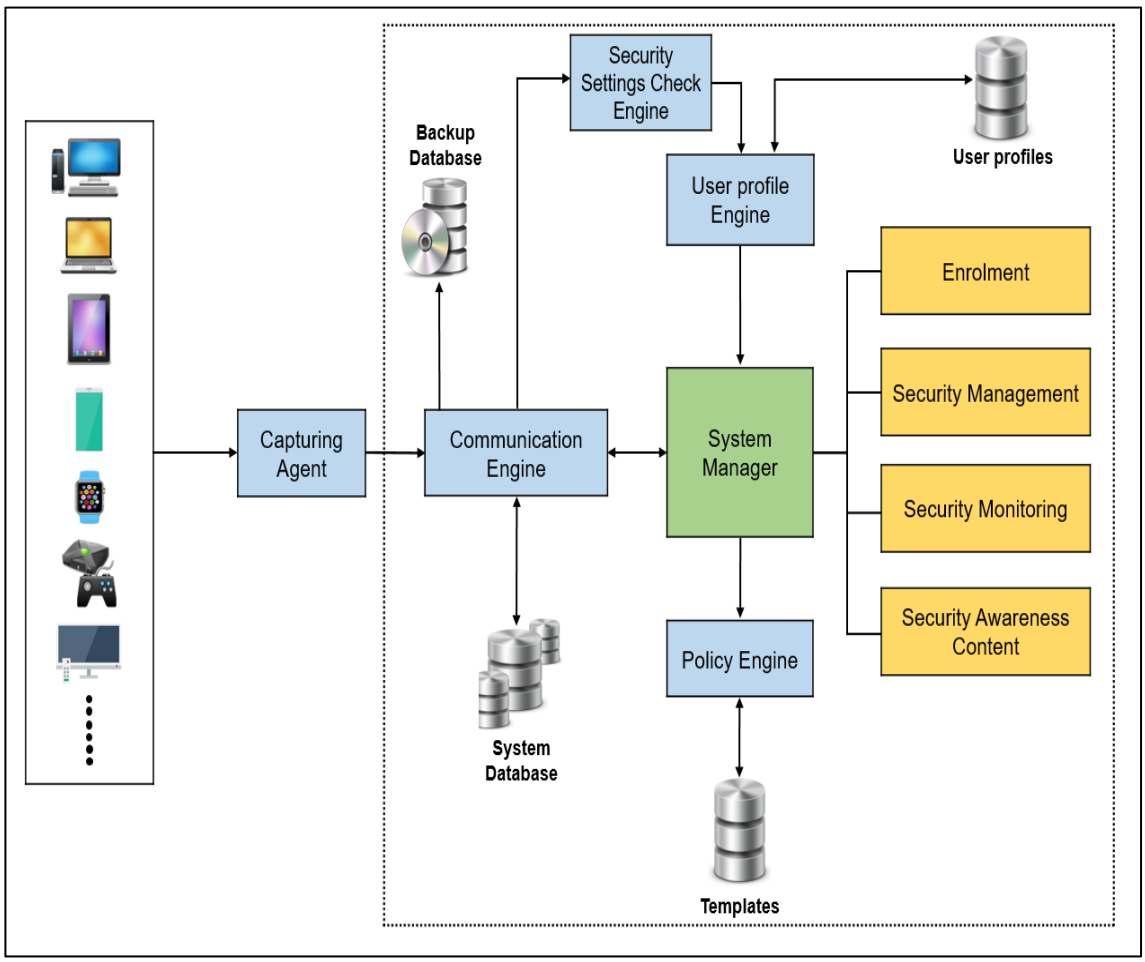


Figure 8.1: Overall System Architecture

The following sub-sections explain in detail the components required to be used in the architecture in order to fulfil its requirements which can make it more effective, practical and convenient.

8.3.1 Capturing agent

The primary role of the Agent is to scan, check, capture the required security information of security controls and settings which are configured in the user's device. In addition, it is responsible for delivering the messages and notification form the system to the users. Due to the variety of technologies, two types of agents are introduced: individual and network-based agent. The individual agent can be installed on the devices which are applicable such as computers and smartphones. However, there are some IoT devices which are not applicable to install any types of applications such as smart fridge and smart light. A network-based agent can be used to monitor and check the traffic of these devices and get the required information.

The main duty of the agent is to provide communication between the devices and the policy manager, including scan, check, capture the required security information of security controls and settings which are configured in the user's device. In addition, it is responsible for delivering the messages and notification form the system to the users.

To avoid any security issues or concerns regarding the collection process and the type of security information, the data collected by the agents is general and does not have any confidential information. For example, the agent can check the password configurations such as password length and complexity without knowing and compromising the configured passwords. Table 8.1 shows how the required data will be collected, proceeded and stored in the proposed framework.

Security settings/controls	Types of retrieved data	Example
Enabling password	Status	Enabled
Minimum Password Length	The number of characters	8 characters
Password Complexity	Enabled/ disabled	Disabled
Enforce Password History	Number	4 password remembered
Antivirus	Status	Enabled
Firewall	Status	Disabled

Table 8.1: An Example of How The System Collects The Required Data

8.3.2 Communication Engine

The main duty of the Communication Engine is to provide communication between the stored data and the main components for the system framework. The data captured by the agents are sent to the Communication Engine in order to be stored securely in the system database. The security information will be retrieved by the Communication Engine to be sent to the Security Settings Check Engine, once the data is stored in the database. In addition, the stored data will be sent to the System Manager via the Communication Engine. Another task performed by the Communication Engine is to enable the System Manager to send the end users some commands (e.g. new enrolment), notifications (e.g. the status) and some awareness contents.

8.3.3 System Manager

The system manager is the main component in the information security management architecture. Its core duty is to enable the user to conduct and achieve a range of different tasks and functions which can be provided by the system. Two different views are offered in the system to the users: administrator and end-users (home users). Nevertheless, the administrator users are given more administrative abilities and duties than end-users. As illustrated in Figure 8.2, the administrator is granted high-level administrative abilities in order to conduct some administrative tasks. In addition, user's profile can be created,

edited and deleted by the administrator. In addition, the administrator can edit and delete the current security policies or add new policies. Moreover, the security awareness contents can be created, reviewed, edited and deleted by the administrator. Furthermore, the administrator can monitor and check the security compliance for the users and devices. On the other hand, the end-users can start the enrolment process for new devices, the request will be pending until it is approved by the administrator. Moreover, the profiles of the managed devices can be viewed by the end-users with the following elements: viewing the policy compliance, viewing the security awareness content, applying an automatic reconfiguration when it is required.

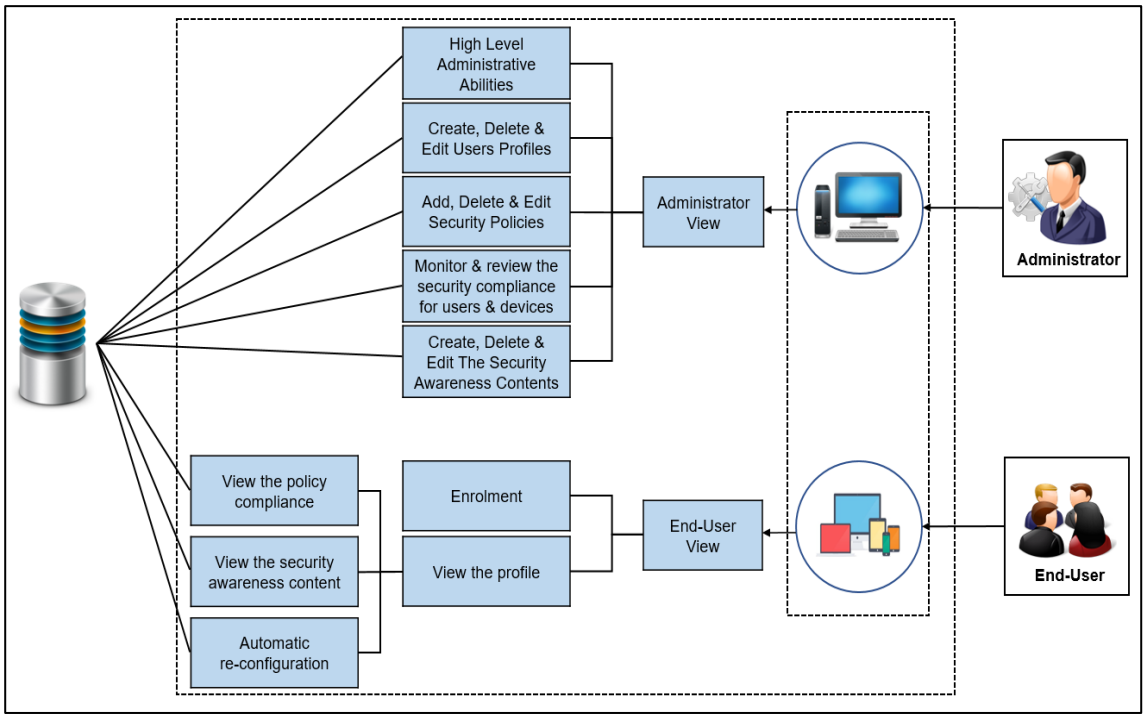


Figure 8.2: System Manager

8.3.4 Security Settings Check Engine

Once the required information about the security settings is captured by the Capturing Agent and stored in the database via the Communication Engine, the Security Settings Check Engine will review and check the extracted security information and compare it

with the assigned policies in order to check whether the device is compliant with the assigned policies or not. Next, the compliance status and the required information will be sent to the user profile. These processes need to be done continuously in order to update the user profile with accurate information.

Table 8.2 shows an example of how the settings of the password policy configured in a computer will be compared with the assigned policies in the system in order to check the security compliance.

Password Policy	The device's Configurations	The Assigned Policy	The compliance Status
Password	Enabled	Enabled	✓
Minimum Password Length	8 characters	12 characters	✗
Password Complexity	Disabled	Enabled	✗
Enforce Password History	4 passwords remembered	4 password remembered	✓
Account lockout duration	Enabled:10 min	Enabled:10 min	✓
Account lockout threshold for Invalid logins	Disabled	5 Invalid login attempts	✗

Table 8.2: The Process for Checking The Security Compliance for Password Policy

8.3.5 The Policy Engine

The key role of the policy engine is to provide a variety of different security policy templates for different technologies in order to be used by the System Manager Engine in order to create a new user profile or update the current one. As disused in Chapter 5, the security settings and controls in several devices including, but not limited to, computers, laptops, smartphones, smart TVs have been reviewed and categorized into several groups based on technology types. For each technology group, a number of security policies

which have been already proposed in Chapter 5 will be applied in the proposed approach in order to monitor and manage the security configurations for different technologies at homes.

8.3.6 Information Security Awareness Contents

As mentioned before that the system is not only proposed to manage the security settings and controls but also to enhance security awareness and knowledge about different threats and issues. As the result shows in the previous chapter that there is a positive correlation between the security concern, knowledge and management. Therefore, the tool will try to raise the user's concern about different types of threats and increase the user's knowledge about different security aspects. In addition, there a positive correlation between the level of technical experience and the level of security concern, knowledge and management of different security settings. As a result, the security awareness messages and contents in the user profile on the client side should be tailored based on the user's knowledge and current needs. The system tries to deliver the awareness contents based on the level of the user's technical experience and the current needs as the following:

- **Novice users:** as it was approved in the previous chapter that novice users have a noticeable lack in the level of security concerns and knowledge about different security aspects which might not enable them to manage their security controls properly. Therefore, the security awareness contents to raise security concerns and knowledge are designed to be general and cover different security threats and aspects regardless of the current issues found in the policy compliance. However, some advice and tips will be offered for each security configuration that the users are not complying with the assigned policies in the user's profile. In addition,

novice users can be provided with automatic troubleshooting and fixing for the current issues.

- **Intermediate and expert users:** as the results show in the earlier chapter that intermediate and expert users have a better level of security concerns and knowledge than the novice users. Therefore, the security awareness for the intermediate and expert users is designed and presented based on the current experienced issues or threats. For example, if the user does not have anti-virus protection in his device, the sections the awareness contents section will deliver information about the importance of the antivirus and the risk of viruses. In addition, more tips and instructions will be presented under each issue in the user's profile.

8.3.7 System Flowchart

Figure 8.3 below presents the process flow which can be taken by the end-users in the proposed system. In the beginning, new users will be asked to register and enrol their digital device and select their appropriate policies in order to create their profiles. After login, the system users are able to view and check their profiles. Several tasks can be performed from accessing the profiles. First of all, users are able to edit their profiles by implementing different tasks. New digital devices can be registered and added in the user profile or removing an existing enrolled device. In addition, the security policies and security level can be reconfigured and updated in the user profile

In addition, users can check the status of their devices security and the compliance of their digital devices with the assigned security policies. Next, users can check the current issues with their security policies and read the tips about how to fix these issues in order to

mitigate the current issues and improve their information security management and awareness.

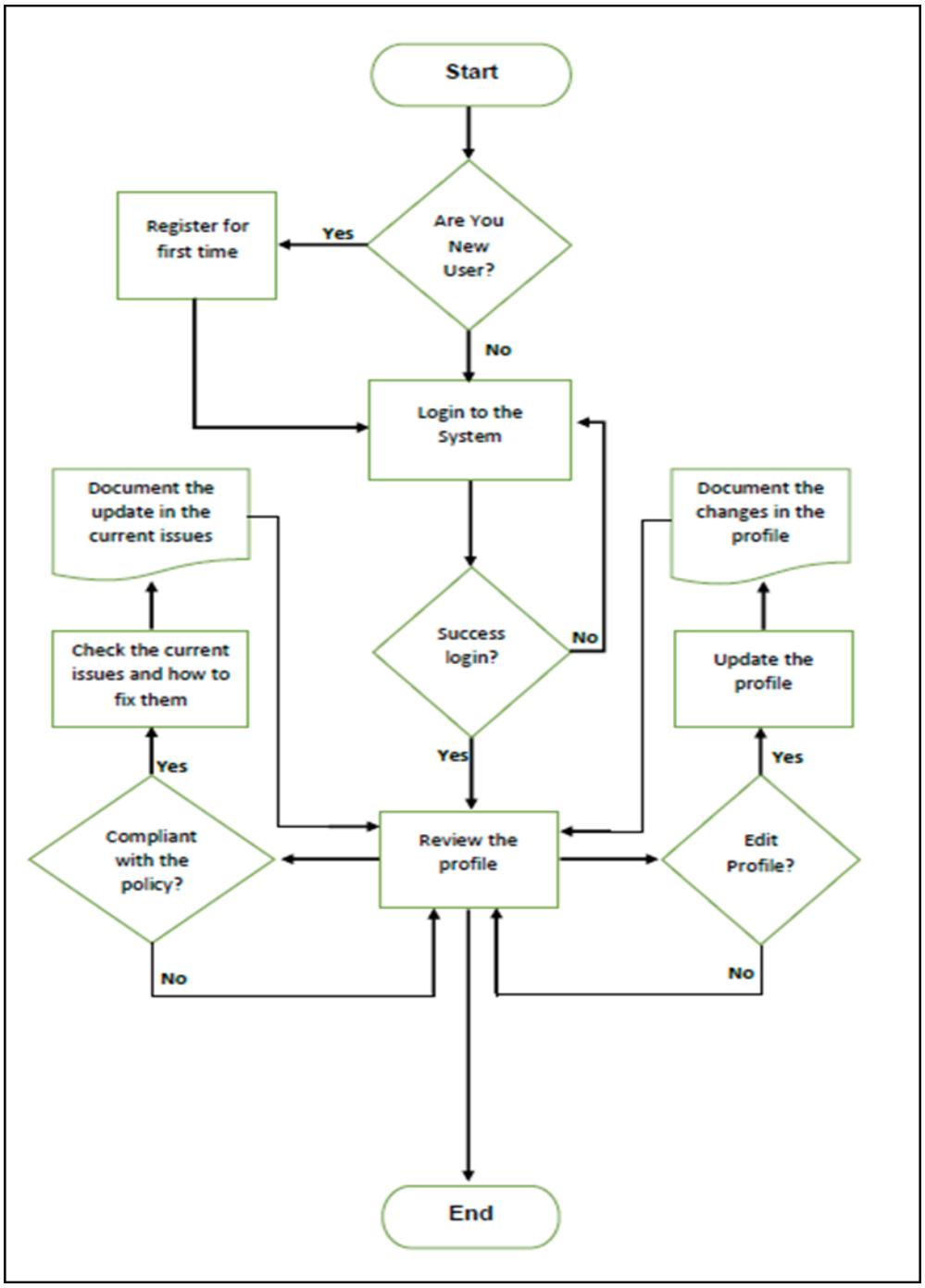


Figure 8.3: A Flowchart of the Proposed Framework

8.3.8 Threat Model

Garg and Kohnfelder developed a model of threats called STRIDE for recognizing threats of computer security (Shostack, 2014). It provides the process of threat modelling and helps in finding threats which can be experienced by computer systems. STRIDE categories threats into six groups: spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege. Shostack (2014) proposed a STRIDE threat model, including the corresponding elements which need to be maintained such as definition, typical victims and examples:

1. **Threat:** Spoofing:
    - **1.1. Violated:** Authentication
    - **1.2. Definition:** Spoofing attack pretends to be identified as another user or trusted source.
    - **1.3. Typical victims:** Processes, external entities and people.
    - **1.4. Examples:** Falsely pretending to be Apple.com or President Trump.

2. **Threat:** Tampering:
    - **2.1. Violated:** Integrity
    - **2.2. Definition:** Unauthorised changes of data stored on network or devices.
    - **2.3. Typical victims:** Data stores, data flows, processes.
    - **2.4. Examples:** Modifying the system database by adding or removing the contents.

3. **Threat:** Repudiation
    - **3.1. Violated:** Non-repudiation
    - **3.2. Definition:** Denying or contest that you did something.
    - **3.3. Typical victims:** Processes.

3.4. Examples: When a user said that he did not order the item or apply changes in a system

4. **Threat:** Information Disclosure
   - **4.1. Violated: Confidentiality**
   - **4.2. Definition:** Exposing information which needs to be kept secret.
   - **4.3. Typical victims:** Data stores, data flows, processes.
   - **4.4. Examples:** Allowing attacker to access files, emails or system database.

5. **Threat:** Denial of Service
   - **5.1. Violated**: Availability
   - **5.2. Definition:** Disturbing or interrupting devices or resources which can provide online services.
   - **5.3. Typical victims:** Data stores, data flows, processes.
   - **5.4. Examples:** An attack seeks to make the system resources unavailable to the main stakeholders.

6. **Threat:** Elevation of Privilege
   - **6.1. Violated:** Authorisation
   - **6.2. Definition:** Enabling an unauthorised user to do some activities.
   - **6.3. Typical victims:** processes.
   - **6.4. Examples:** Enabling normal users to perform some activities and tasks as administrator.

Several assumptions of STRIDE threat model are made to discuss the threats against the proposed approach:

- **Spoofing:** login credentials can be stolen or hacked which can be used by attackers to login to the system in order to access the system data and confidential information.
- **Tampering:** some alterations can be done by unauthorised individuals on the data of files which are being sent to the users or stored in the system databases.
- **Repudiation:** users can deny that they did some changes or requests. The system log service can help in preventing these types of threats.
- **Information Disclosure:** Confidential information and data which are stored in system database can be exposed. This can be mitigated by implementing Access Control Lists (ACL) to protect the database and enhancing OS security by applying some security features such as encryption.
- **Denial of Service:** the front-end of the system can receive a huge number of constructed requests at the same time which can make the network connection flooded with massive amount of data and packets.
- **Elevation of Privilege:** this can happened when an attacker exploits a design flaw, bug or an error in the configuration of the system for gaining access to the system resources in order to get confidential data, install malware or run malicious command.

8.4 Operational Considerations

The proposed approach aims at improving information security management and awareness for home users across different devices and technologies. Nevertheless, a number of issues and concerns need to be considered and resolved in order to make the proposed system work effectively:

- **Integration and compatibility:** the proposed framework needs to interact with several digital devices and technologies. Therefore, it is important for the policy system to have the ability to integrate and interact easily with different types of data

and settings. In addition, the system should be able to be capable and compatible with several devices and operating systems such as Windows, IOS and Android.

Therefore, several application programming interfaces (APIs) need to be considered and used in order to allow the proposed solution to communicate and interact with different digital devices in order to collect the required data and feed the proposed approach. Each operating system has its own APIs which can enable the proposed system to capture the aforementioned information. For example, The Android SDK has several classes for settings such as:

- **Class Settings.Secure:** it contains system preferences that applications can only read without the ability to write. These are for preferences that the user must obviously change through UI of the system or specific APIs for those values which cannot be amended directly by applications.
- **Class Settings.Global:** it contains preferences which can be always applied identically to all users which can be read by applications without the ability to write. These are for preferences that the user must obviously change through UI of the system or specific APIs for those values which cannot be amended directly by applications.
- **Class Settings.System:** it contains mixed system preferences. The table includes simple name/value pairs which can be used to access different individual settings entries.

For example, the following methods in the above classes can be used to obtain different data.

- The `getInstalledApplications` of the `packageManager` can be used to retrieve all the installed applications.

- The `packageInfo` and `versionCode` can be used to check if all the installed application are updated.
- The `KeyguardManager` can be used to check if the device is secured with a PIN, Patter or password.
- The `INSTALL_NON_MARKET_APPS` Of `Settings.Secure` can be used to check if the device is allowed to install non-market applications.

- **Privacy and Security:** from the end user perspective, privacy is an important aspect which needs to be considered as the proposed system aims at managing information security and controls in the digital devices. The storage, process and communication in the proposed system must be achieved in a method that can reduce any possible threats such as interception or misuse the stored information. The proposed architecture must be designed properly to have the ability to separate the activities and duties, apply encryption and take protective actions against for securing the access to the stored sensitive data. Therefore, an encryption method such as the Pretty Good Privacy (PGP) can be used in the client side in order to mprovide more security for the data communication. In addition, the Secure Socket Layer (SSL) can be used to send the encrypted collected data from the client to the main server. Privacy can also be protected in the proposed architecture by collecting and using only the information which is required for the system process. For example, the proposed system must only have the ability to know if the PIN is enabled in the device without being able to know the actual PIN.

- **Battery life:** battery consumption and life is a critical issue experienced by digital device users. Digital devices cannot offer any functionality without power. Therefore, the proposed system needs to avoid consuming the battery life by considering

different principles and methods. The operations and activities in the proposed system should be reduced and optimised. For example, instead of re-downloading the data and waking up the device, the system can cache the downloaded data in order to save the battery life. In addition, the unnecessary actions in the proposed system can be delayed until the device is charging.

- **Scalability and Response Time:** Due to the mechanism of the proposed system which will collect data from devices and store it in a central server, several issues should be considered such as synchronization with the agents in different devices and different users. The process of checking and capturing the required data from the devices should be undertaken continuously in order not to leave the user waiting for a long time.

8.5 Mock-up Design

After presenting a theoretical explanation of the proposed framework used for improving the security management and awareness for home users in the previous section, the next stage of the research focuses on developing a mock-up design that simulates the proposed model. A mockup design has been selected and used for the simulation in the research with interactions applied in many objects in order to enable them to respond to a variety of triggers. Several scenarios were assumed, designed and used during the simulation process for many reasons. First of all, it helps in demonstrating and visualising the real system for managing and monitoring information security for home users. This will allow the main stakeholders to understand the functionalities of the system and how it is supposed to work. In addition, it enables the stakeholders (end-users and experts) to test the usability and functionality early in the development process. Moreover, it helps in

acquiring feedback from users about the proposed system. Moqups app web was selected to develop the prototype design.

In the proposed mock-up design, the main menu has been designed to be accessible by the administrator from each section or component. In addition, the visual icon has been used in the menu in order to make it easy for the administrator to recognise each component and its task. The proposed mock-up design consists of several components and each component has different tasks: Main Dashboard, Enrolment, Management, Policies, Reports and Support.

8.5.1 Main Dashboard

The first interface in the proposed mock-up design is the main dashboard. The aim of the dashboard is to organise data in a way which makes it easy to understand by the users. This helps to monitor all the home digital devices in a usable and cognitively effective manner. The dashboard is designed to provide information about the home devices such as settings alerts, the status of the enrolled users and their managed devices, statistical information about the status of the devices and their compliance with the assigned policies as shown in Figure 8.4. The non-compliant settings and devices are coloured in red and compliant settings are coloured in green in order to attract the administrator's attention in a usable method. In addition. Several sections and competent are demonstrated in the dashboard but not limited:

- **Security Settings Alert:** it shows the current status of several security settings in the managed devices.
- **Activity Feed:** it displays a list of recent activities performed in the system and the managed devices.

- **Security Compliance by Users:** it includes the compliance status of all the digital devices owned by each user.
- **Security Compliance By Devices:** it presents the compliance status for each individual device.
- **Security Policies For All The Devices:** it shows the compliance of several security policies for all the managed devices.

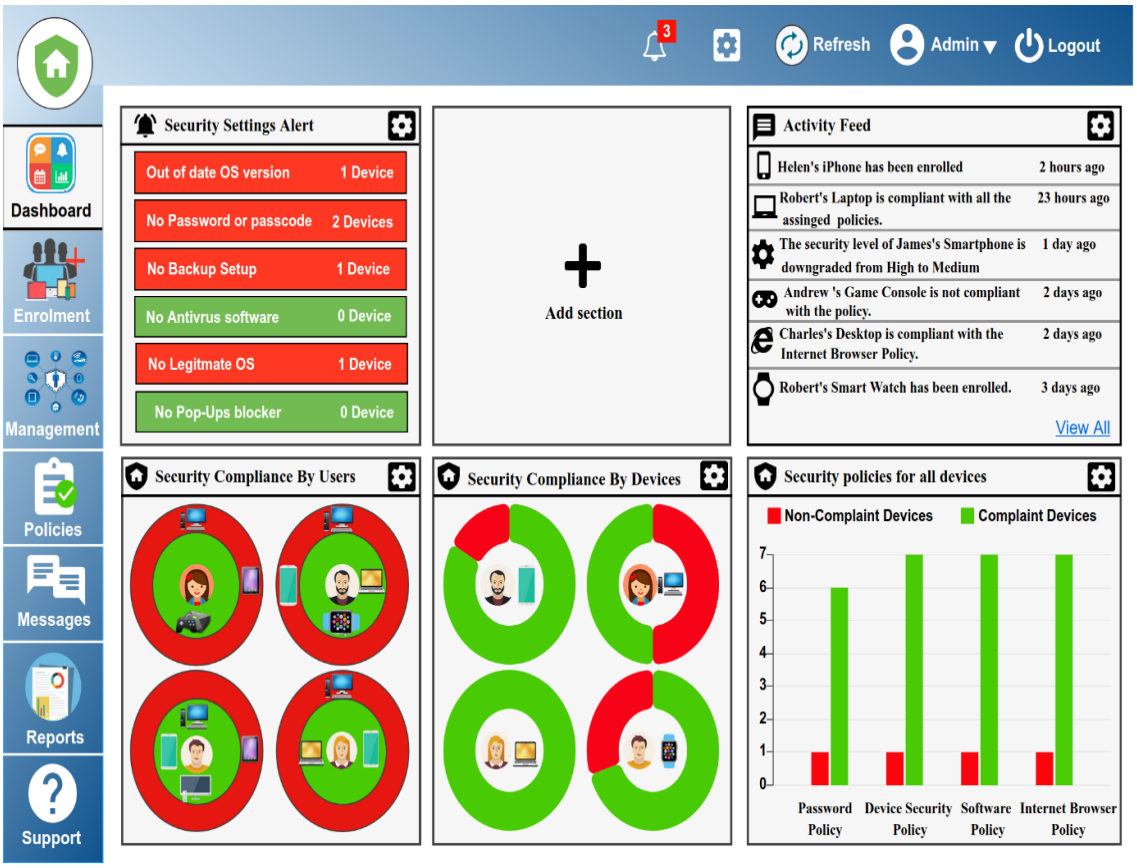


Figure 8.4: The Main Dashboard for Administrators

As already mentioned that the proposed tool needs to be usable and flexible in order to be effective and achieve its goals. Therefore, the administrator can have the ability to add new data in a specific section a shown in Figure 8.5. The selected data will be shown in the sub-window in order to make it easy for the administrator to see how the new data will be presented in the new section.

Figure 8.5: Adding a New Section in The Dashboard

In addition, Figure 8.6 shows that the dashboard layout and format can be changed based on the administrator's needs from the settings section in top menu which can make the system more usable and flexible.

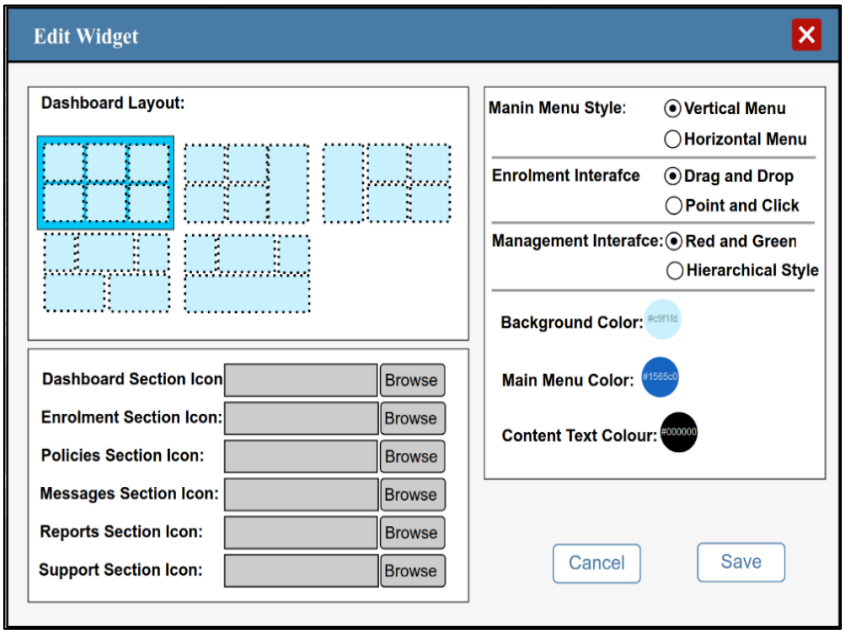


Figure 8.6: Changing The Layout and The Format

In addition, the administrator can have the ability to change any section with different data or different style of presentation as illustrated in Figure 8.7, this can give the administrator more flexibility to change the data based on his current needs.

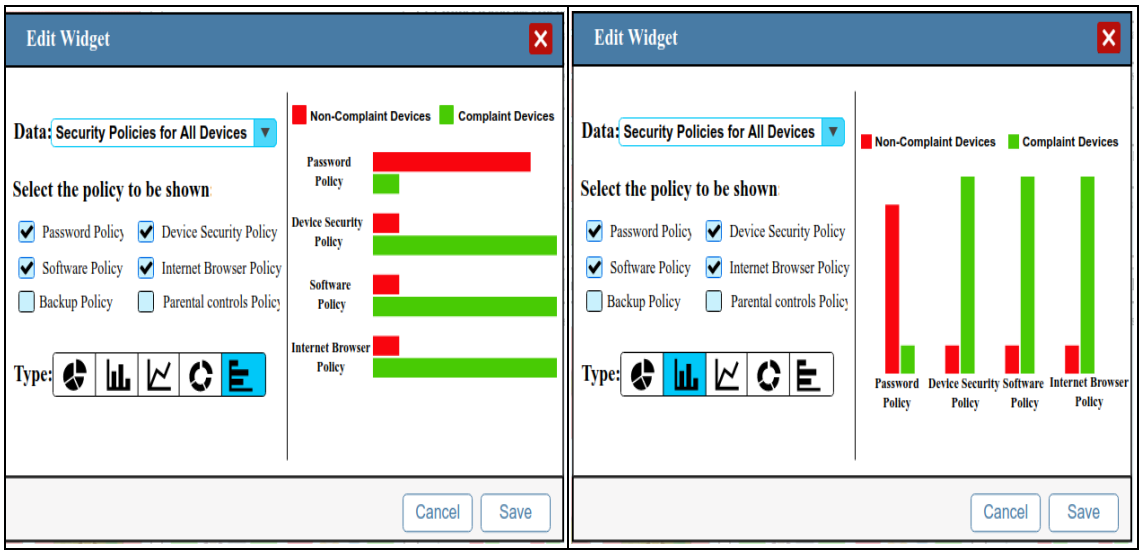


Figure 8.7: Changing The Assigned Data or Presentation in a Section

8.5.2 The Enrolment

The administrator will be notified in the enrolment interface with some detail for each discovered device. This can make the system easy to use and effective in establishing the enrolment process as illustrated in Figure 8.8.

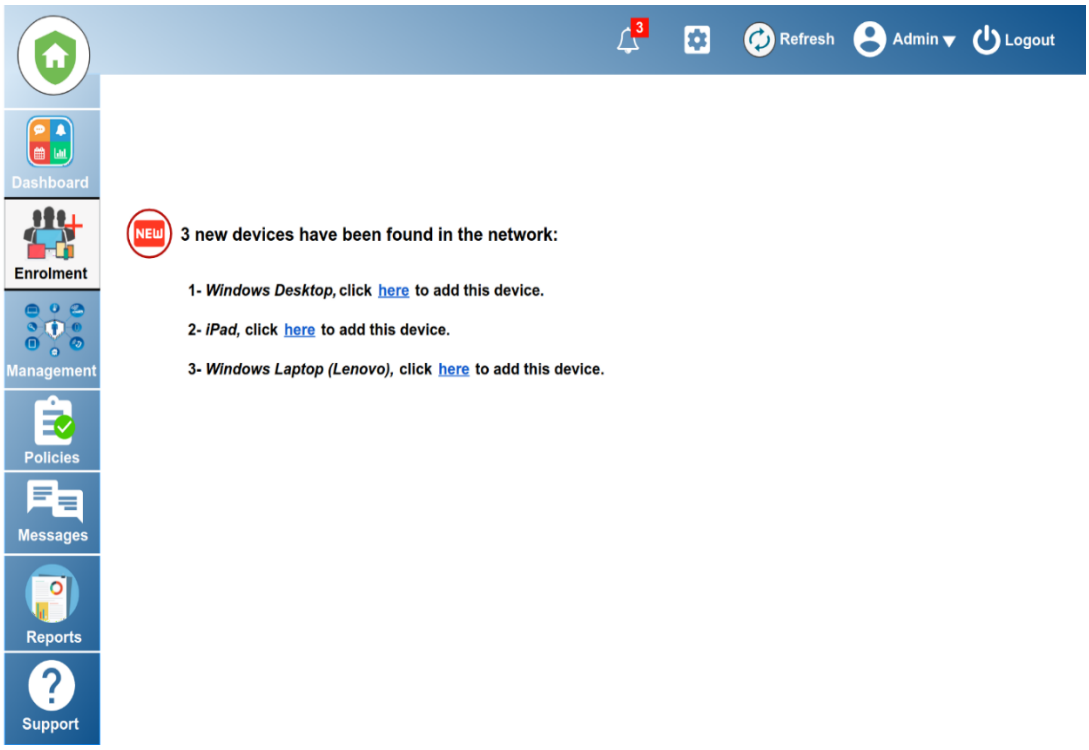


Figure 8.8: The Enrolment Interface for Administrators

The enrolment processes are designed based on the user's technical experience in order to avoid any difficulty and to add more granularity into the system. For example, most of the enrolment processes for novice users are done automatically as they do not have the appropriate skills to get enrolled properly. Figure 8.9 shows the enrolment process for novice users.

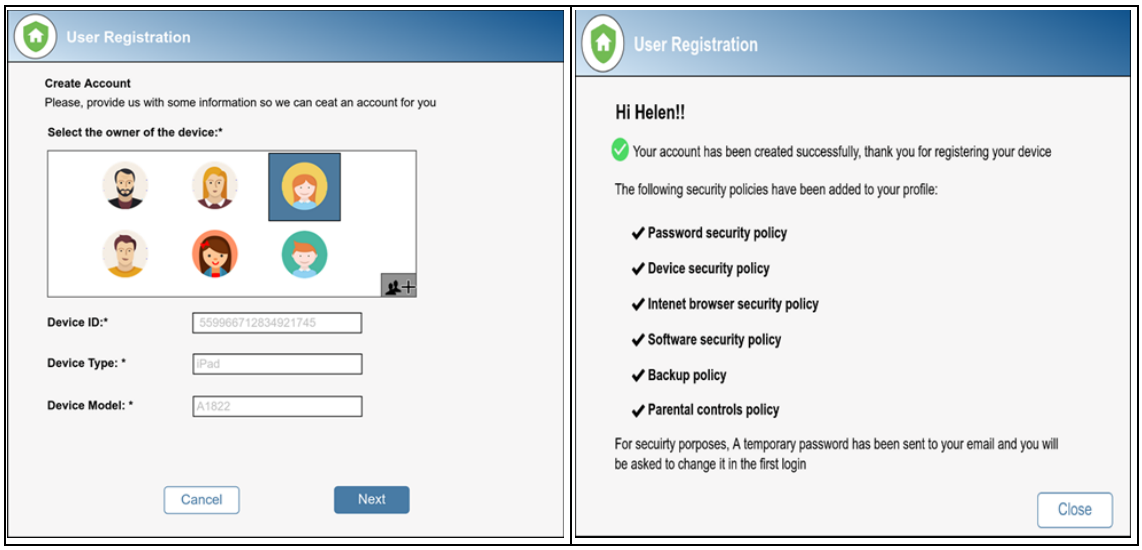


Figure 8.9: The Enrolment Process for Novice Users

It is expected that the intermediate and expert users have good security knowledge and skills as it was shown in the survey's result. Therefore, they can be provided in the system with an option to choose the required security policies and the level based on the current needs as shown in Figure 8.10.

Figure 8.10: The Enrolment Process for Intermediate and Expert Users

If there is a new user needs to be added to the system, the adding users' icon ( ) in the enrolment page can be clicked. Next, the user will be asked to fill some information such as name, email, level of technical skills as demonstrated in Figure 8.11.

Figure 8.11: Adding a New User

8.5.3 The Management

The management section is responsible for managing, monitoring and checking the compliance of the enrolled devices with their assigned policies. The interface is designed as a hierarchical style which can give a panoramic view of all the managed users and their enrolled devices. In addition, Red and green colours are used to illustrate the non-compliant and compliant devices in order to facilitate the administrative tasks as shown in Figure 8.12. All these features can make the system easier and more flexible.

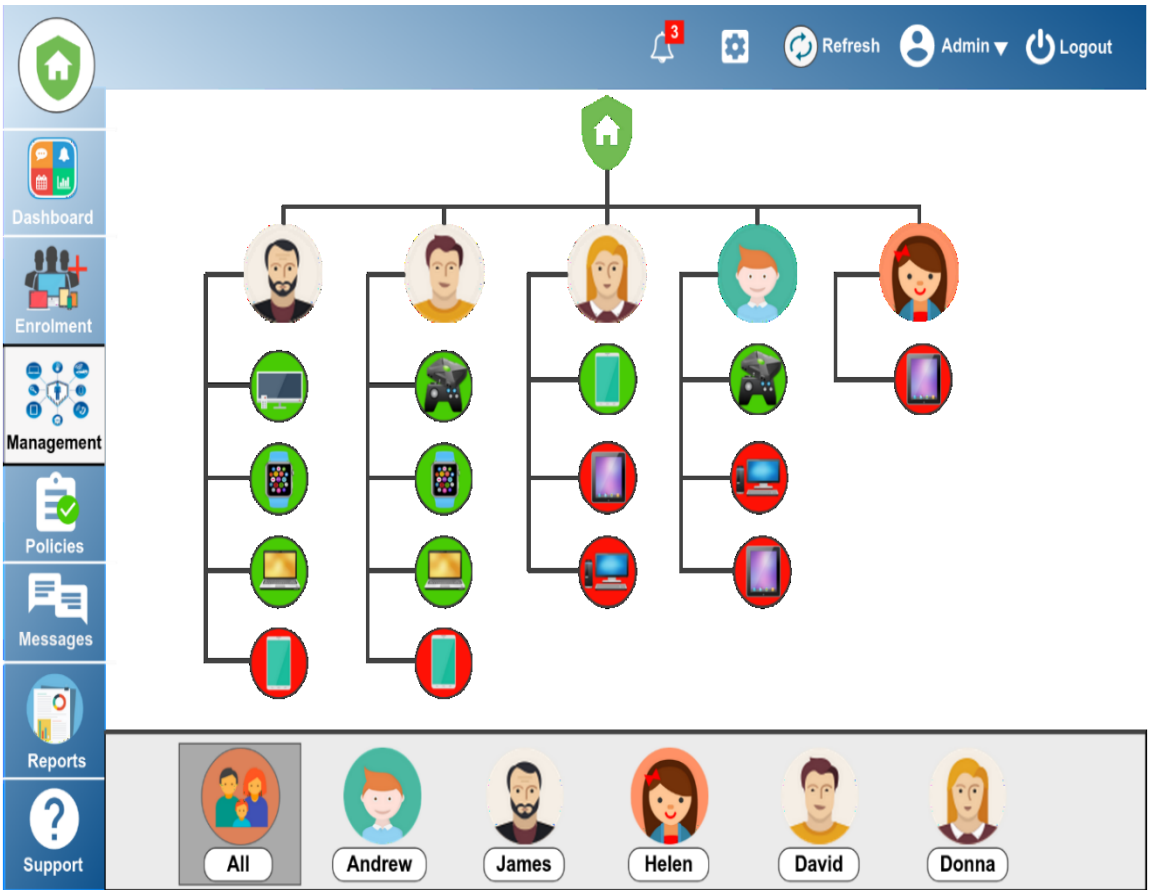


Figure 8.12: The Management Interface for All Users

The administrator can view all the users together by selecting “All” or a specific user can be only displayed by clicking on the specific name and the rest of the users will be blurred as shown in Figure 8.13.

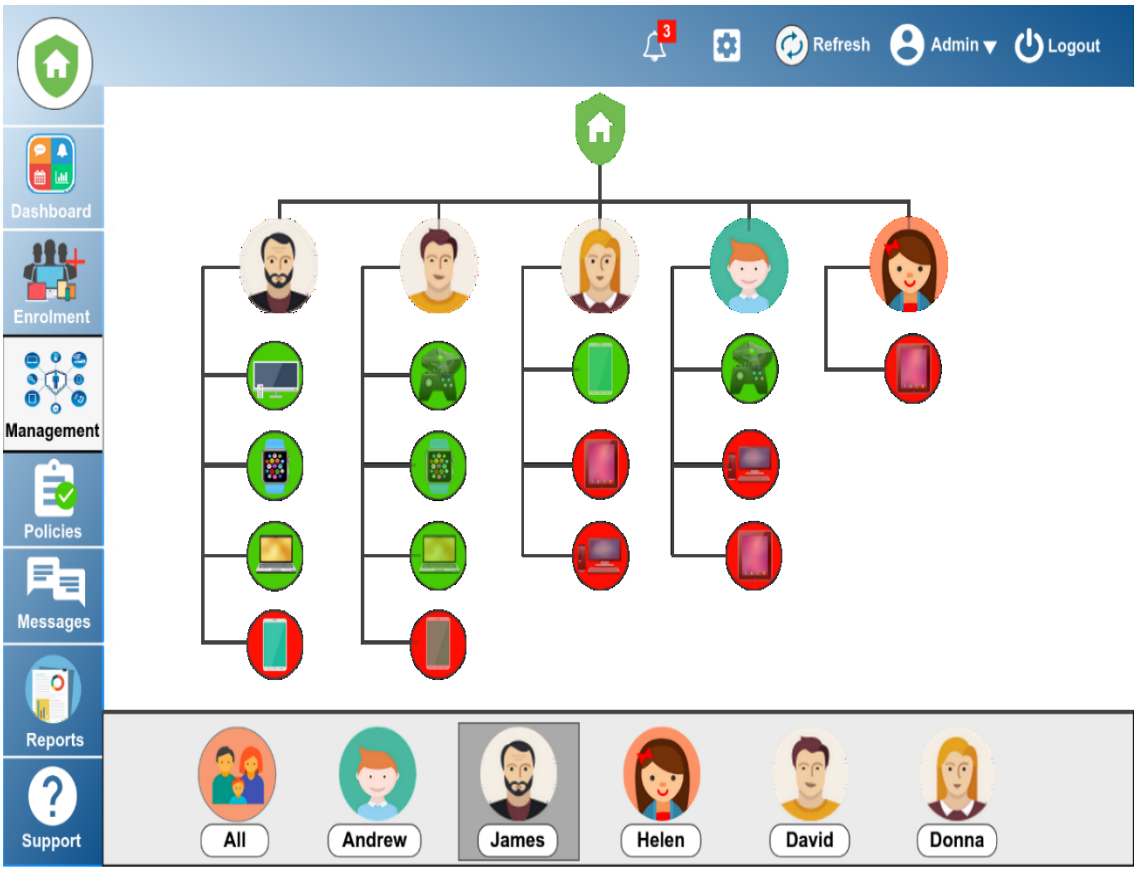


Figure 8.13: The Management Interface after Selecting a Specific User

A description box can be displayed when the administrator does a mouseover on a specific device, which provides some information about the device as shown in Figure 8.14. The box border is coloured in green or red in order to attract the administrator's attention. In addition, this can make the management procedures and processes are easy and convenient for them.

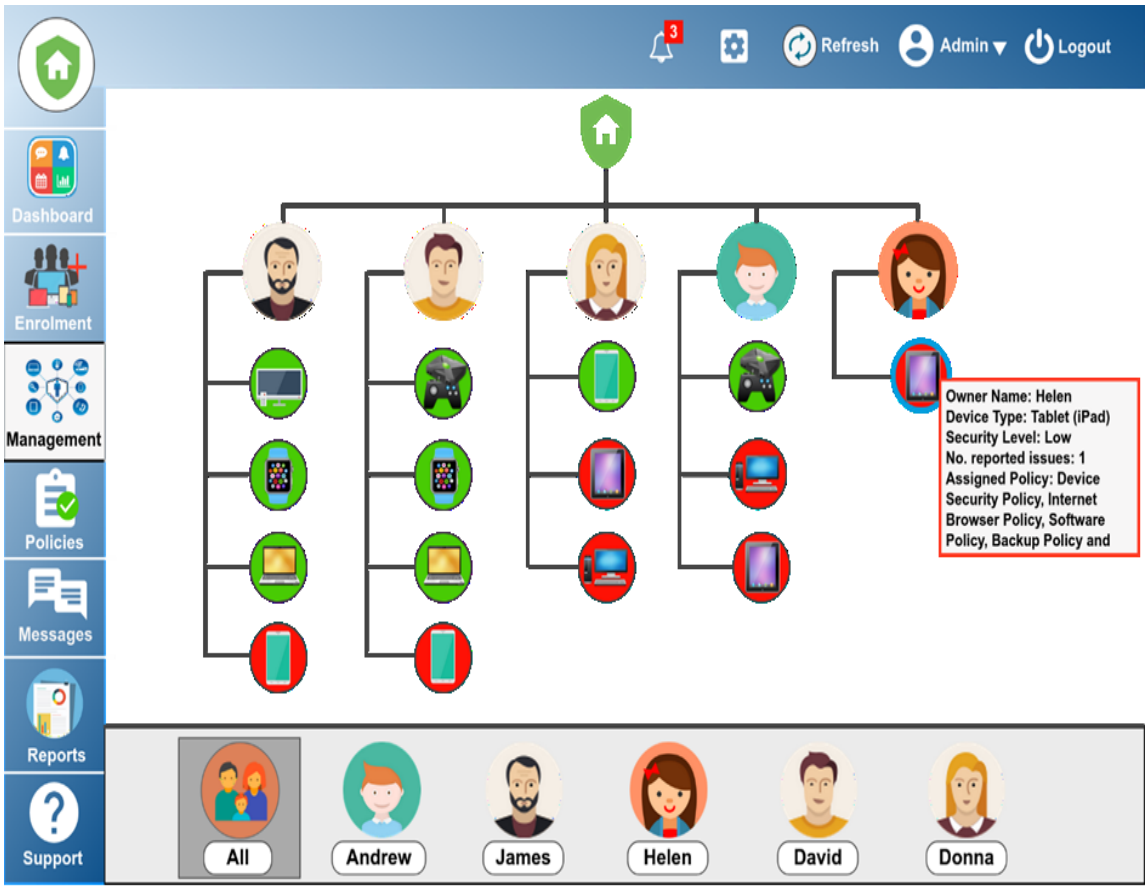


Figure 8.14: Mouseover Information about a Specific Device

In addition, more options can be provided to the administrator such as viewing profiles, changing the owner, sending messages to the users and removing the devices as shown in Figure 8.15. This can add a good enhancement in managing the tool effectively make the process of the management easy for administrators.

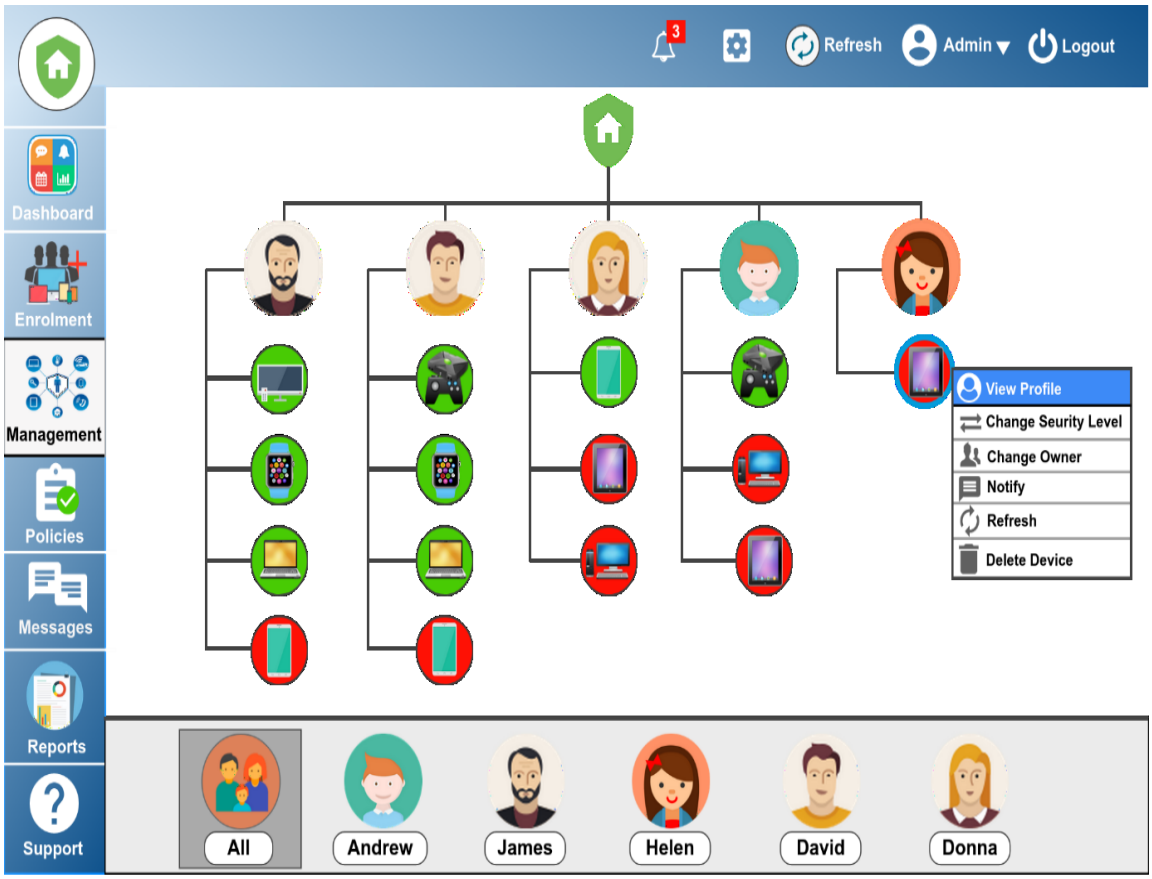


Figure 8.15: Right-Click Option in The Management Interface

8.5.4 The User Profile (for administrators)

The administrator is provided with a comprehensive profile for the selected user which can show the device compliance in a usable way as shown in Figure 8.16. The policies are designed as a horizontal clickable menu with a green tick and a red cross icon to show the status of the compliance. In addition, the profile includes a recent activity section, a profile summary and the current alerts. Moreover, changing the current owner or the security level can be done via the interface. The whole layout of the profile or a specific section can be changed and customised based upon the administrator's priority in order to achieve the system's goals. In addition, a top menu in the profile is provided for administrators in order to navigate and move easily between the devices owned by one user.

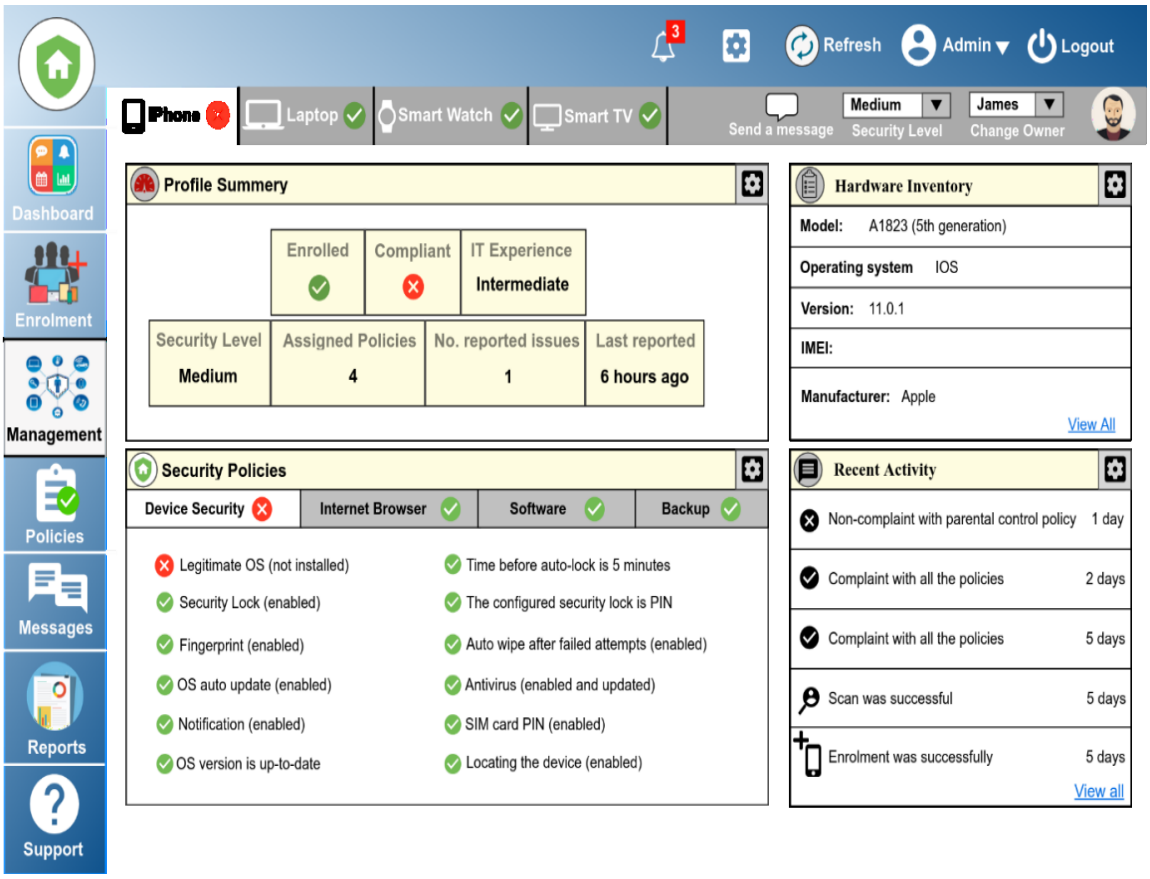


Figure 8.16: The User Profile for One User

8.5.5 The Policies

The administrator is provided with a submenu which allows him to view, edit and delete any policy from the current policies in the system. In addition, a new policy can be added to the system by the administrator as shown in Figure 8.17. This can help administrators in managing the security policies in the system easily.

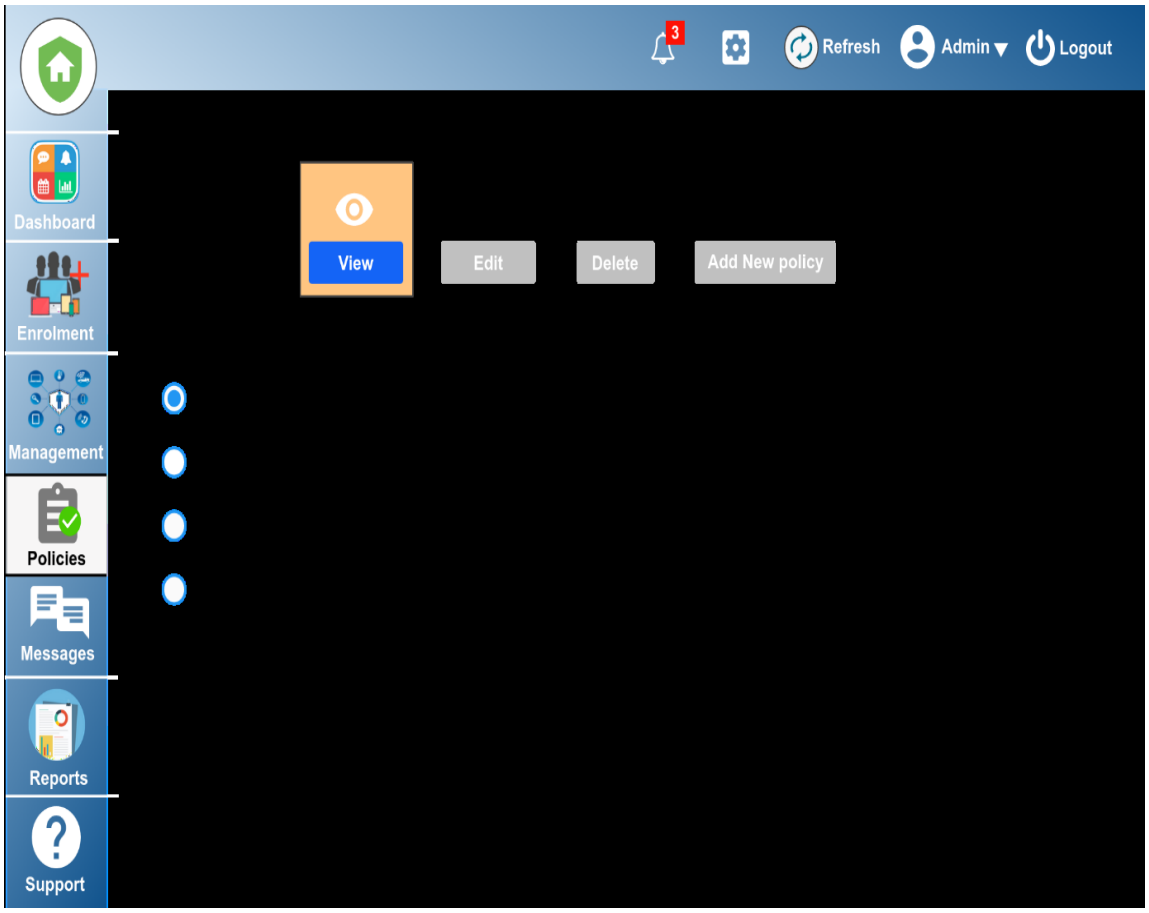


Figure 8.17: The Security Policies Interface

Once the administrator selects a specific policy, and click the view button, the whole sub-policies will be shown as illustrated in Figure 8.18. In addition, the administrator can select a security level to view the configured settings for the selected policies. Moreover, the administrator can get more explanation about each policy statement by clicking on the red information icon beside each statement. The administrator can easily move between the policies by clicking on each one in order to expand and show the policy statements. All these options and features can make the process of managing security policies in the system usable and fixable.

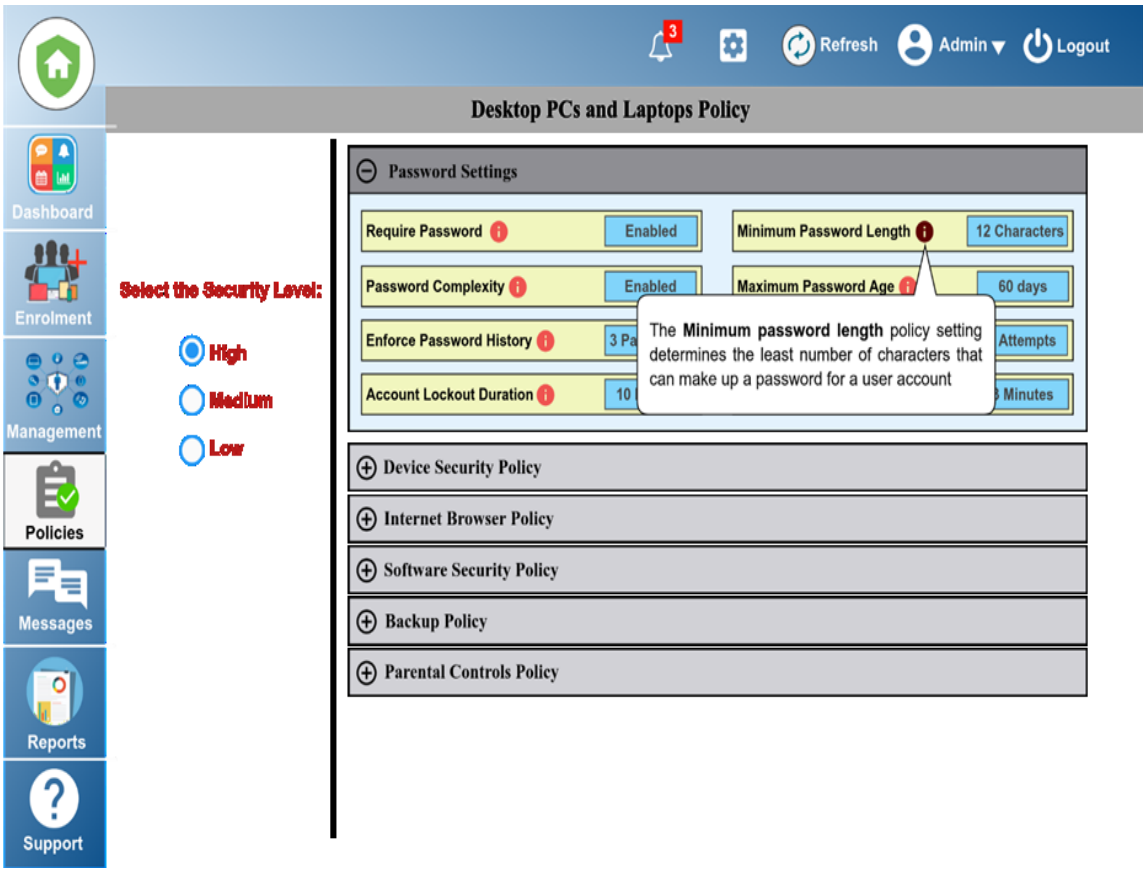


Figure 8.18: Password Policy for Desktop and Laptop Policy

8.5.6 The User Profile (For End User)

Each user is provided with a user profile which contains information about the security status and the assigned policies for each device. The layout of the interface and the added sections can be changed by the user from the setting section. The user profile is designed to notify the user and make them aware of the current issues or potential threats by providing the users with several sections such as the profile summary, recent activity and policy compliance. In addition, the profile aims to enhance cyber security knowledge and awareness for home users. Therefore, Do You Know section provides some statistical incidents which can raise the user's concern in order to enhance the level of security knowledge and manage the security controls effectively as evident in Chapter 7. Quiz section can be provided to increase the user's security knowledge. It can be seen in Figure

8.19 that the user is intermediate and he has one issue in a security policy that he does not have antivirus protection. As a result, the provided information in Do You Know section and the Quiz all is about the importance of antivirus and the virus threats.

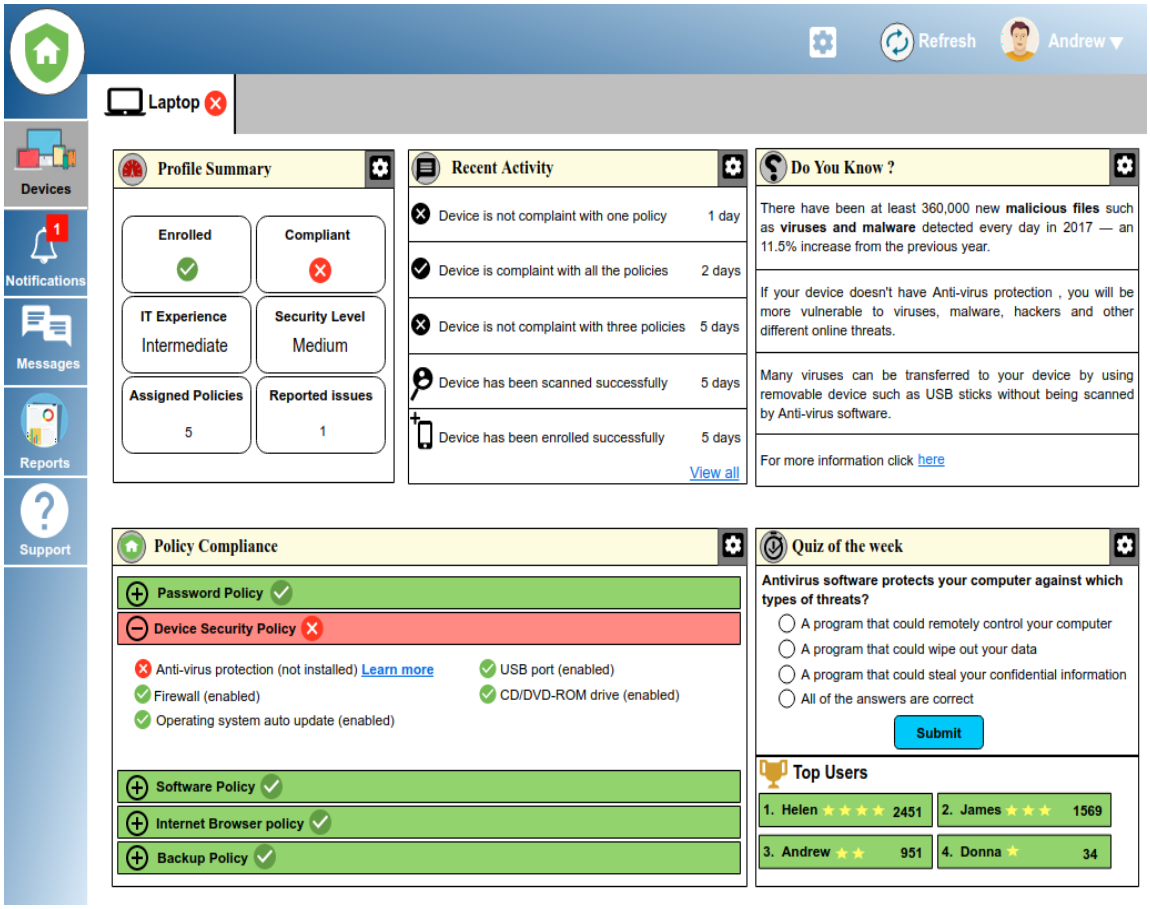


Figure 8.19: User Profile for Intermediate user

On the other hand, if a novice user has an issue in one security policy, Do You Know section and the Quiz section will provide information about different security aspects in order to raise the security concern and knowledge. As shown in Figure 8.20, the user has an illegitimate OS but the two sections still give information and knowledge about many aspects.

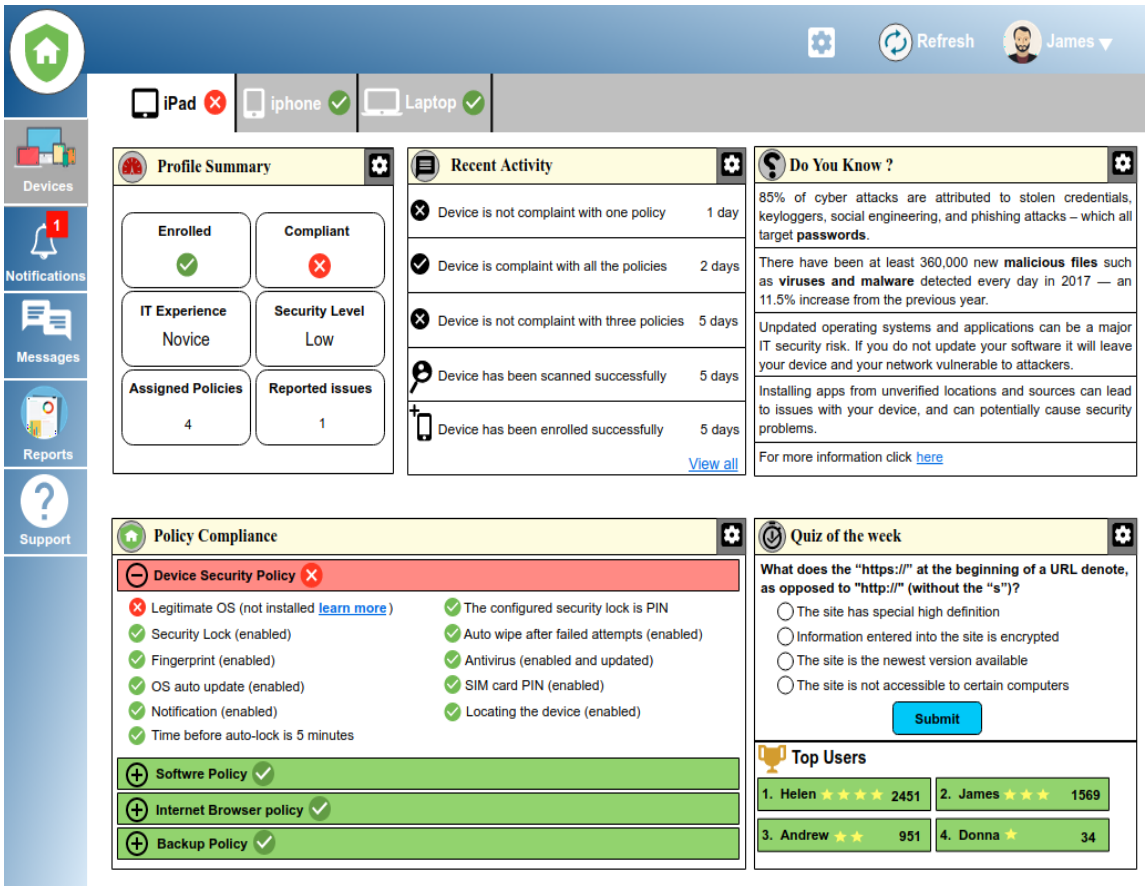


Figure 8.20: The User Profile for Novice User

In addition, users are provided with a link beside each policy statement which has an issue. This link offers the user a window that has more information about the current issue as illustrated in Figure 8.21. In addition, only the novice users are provided with a quick troubleshoot for the current possible threat by doing automatic reconfiguration or installation on behalf of the users who do not have good technical knowledge. In addition, more tips and advice about the current risk is offered in the same window. This can increase the learnability and allow users to gain more knowledge about securing their devices and networks.

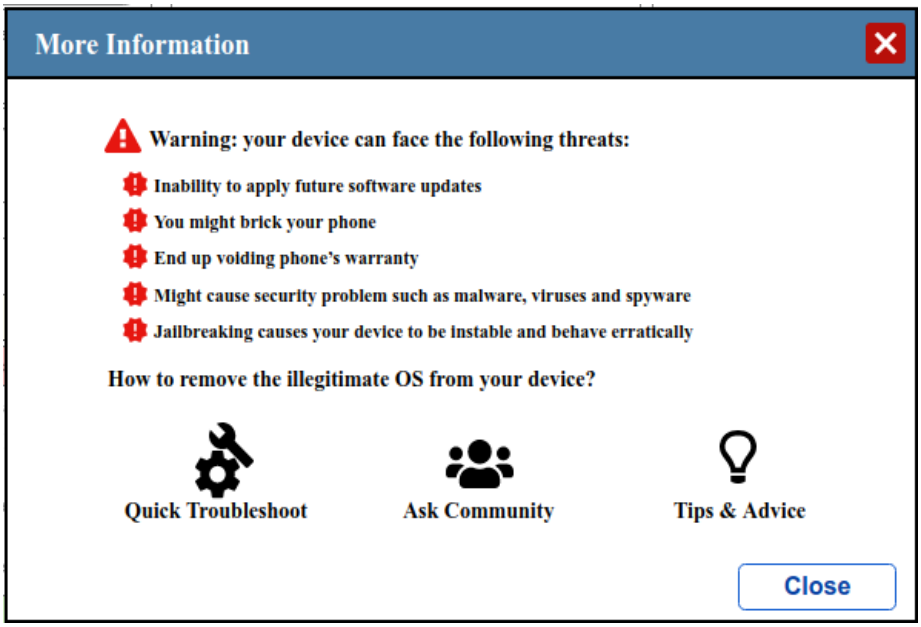


Figure 8.21: More information for Novice User

Another option can be provided for users in the previous interface which is Ask Community option. It is a collaborative website which allows the home users to share their knowledge, experience and advice about a variety of security issues and threats as shown in Figure 8.22. This collaborative website can be hosted and managed by non-profit cyber security orgnisations such as Get Safe Online. It can enable home users to exchange and find security advice and tips easily in order to manage their security controls effectively.

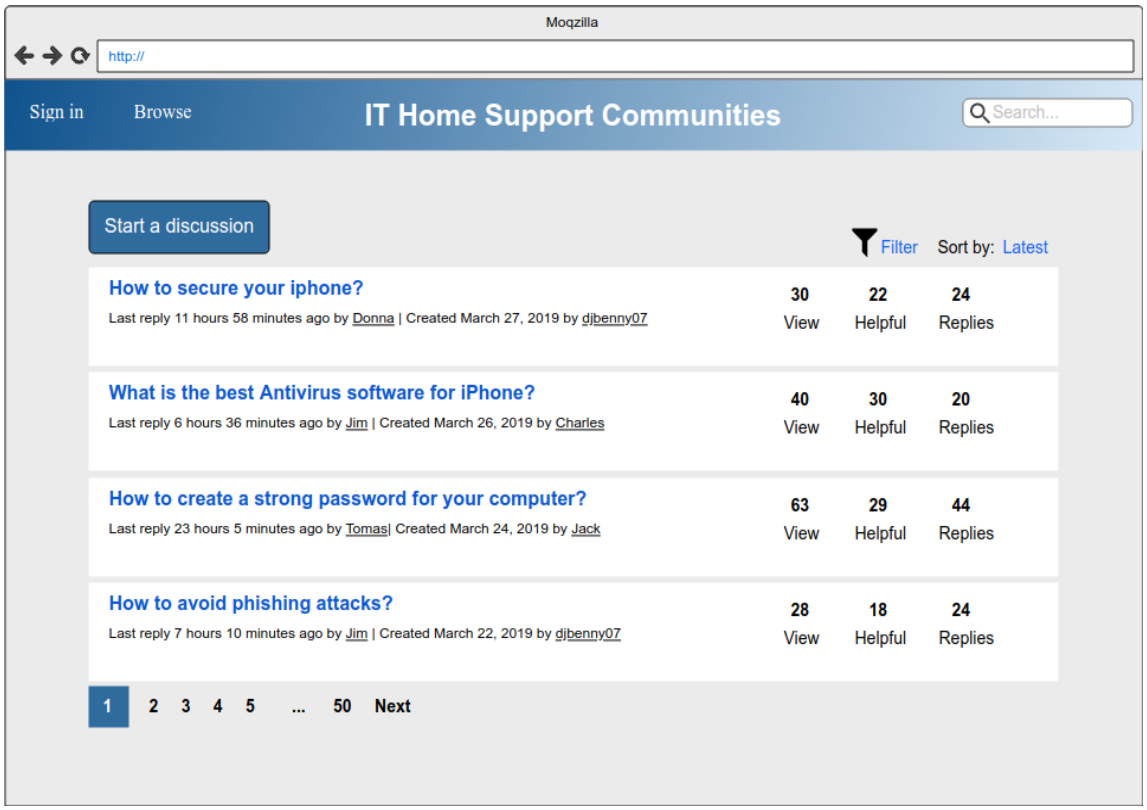


Figure 8.22: IT Home Support Communities

8.5.6.1 Mobile Version

Another version for the user profile is designed for the home users as a mobile version. It includes all the information which have been already discussed in the prior section. As shown in Figure 8.23, the user is offered with some information about his device compliance. In addition, more tips and advice are provided for the users which can help them to fix the current issues and increase their knowledge. Each policy can be expanded in order to check the statements of the assigned policy statements which can make the profile more usable.

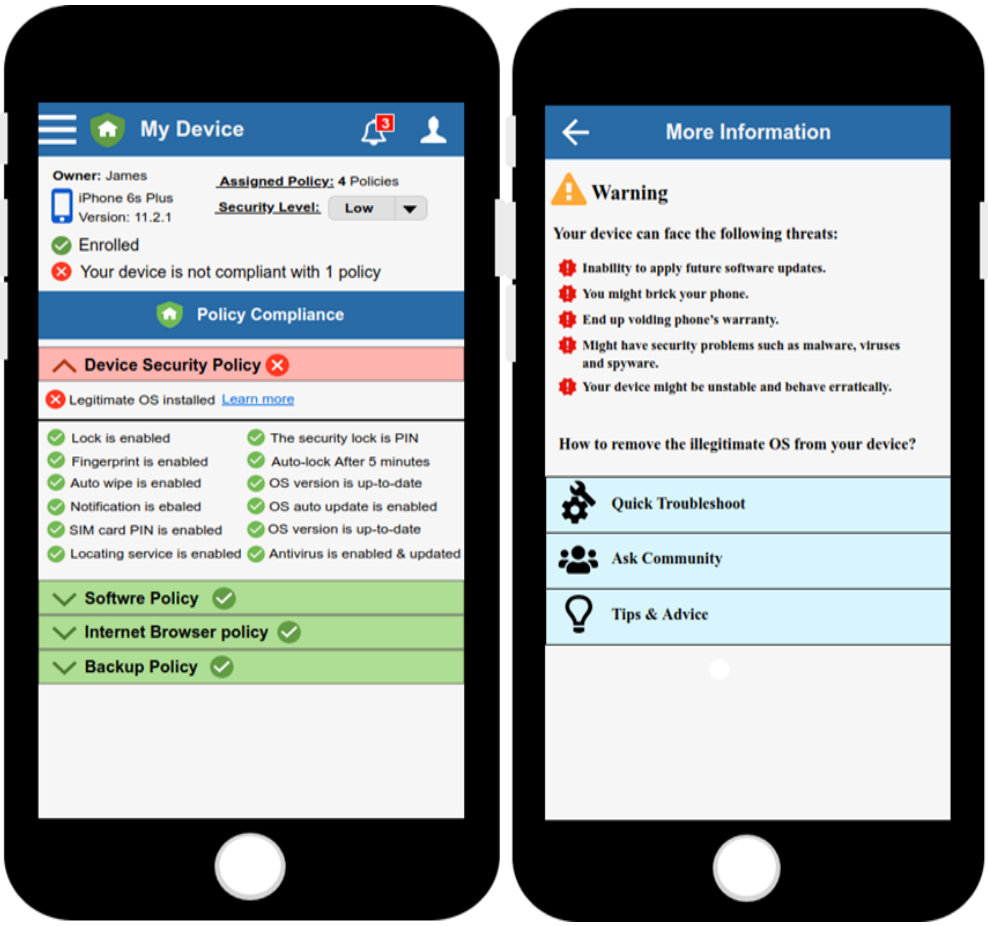


Figure 8.23: A Mobile Version for The End User Profile

8.6 Evaluation of The Proposed Approach

In addition to the mockup design of the proposed framework, a further qualitative evaluation is conducted to gain feedback from end-users and IT security experts. The aim of the focus group method is to evaluate the validation and usability aspects of the proposed framework for improving cyber security management and awareness for home users. In order to evaluate the al the aspects of the proposed framework, two separate groups of stakeholders were selected with two separate sets of information and questions: experts and end-users.

8.6.1 Design and Methodology

At the beginning of the two focus groups, the research introduced himself and the purpose of the focus group discussion. Next, information sheets and consent forms were provided to give them more information about the research. Moreover, the participants were informed that their participation is voluntary and the session will be recorded and their personal information will be kept anonymous and confidential.

The participants were provided with a presentation which includes the framework and the main components and aspects in the proposed approach. Then, a live demonstration for the proposed mock-up design was conducted for each focus group session. The following different scenarios are presented in the two focus groups in order to demonstrate and visualise the processes and tasks which can be performed in the proposed system:

- How all the components and sections can be navigated in the proposed design.
- How the administrator can navigate the components of the main dashboard and how it works by adding new sections or changing data presented in one section.
- How the enrollment process for different users can be conducted in the system.
- How the administrator can navigate the components of the management section including the user profile in the administrator side.
- How the security policies can be reviewed, created and updated in the proposed system.
- How the end users can navigate their profiles and check their status.

8.6.1.1 Experts Focus Group

The main aim of inviting experts in a focus group discussion is to validate the main functionality and feasibility aspects for the proposed approach. The experts were recruited

for the focus groups discussion at The Thirteenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019), July 2019, in Nicosia. The invitations and the selection process have been facilitated by my supervisory team. Initially, 5 participants were invited to the session. However, one participant left the session as he had an urgent duty. Table 8.3 shows a summary of the participants' background and their assigned IDs.

ID	Participants	Location	Gender
A1	Researcher in Information Security	At University	Male
A2	Researcher in information systems and security	At Research Center	Male
A3	Researcher in Information Security and Risk Management	At University	Male
A4	Researcher in IT	At University	Female

Table 8.3: Expert Participants' Background

14 open-ended qualitative questions were provided for the Experts' group. The questions were drafted and reviewed in terms of being understandable and objective in order to achieve the aims of the focus group method:

1. **What are your thoughts on the identified research problem?** The aim of this question was to examine the validity of the research problem and how the experts think about this problem.
2. **How realisable/feasible do you feel this proposed design is at the operational level?** It is important to investigate the feasibility of the proposed framework if it is implemented and applied in a real environment. This question can be answered effectively by information security experts.

3. **To what extent do think the utilisation of the security policies in the proposed approach could enhance the security management and awareness for home users? Is it convenient? Usable?** The concept of security policies is already implemented in organisations. However, an information security management system for home users is a novel approach and has not yet employed within the home environment.
4. **To what extent do you think that the proposed three security levels for the policies could make the system more flexible? More/less levels?** The aim of this question was to find out whether it is a good idea to have three levels of security in the proposed system.
5. **To what extent do you think the proposed design can succeed in providing better security monitoring, security management and awareness in home environments?** If the proposed framework is implemented within home environment, can the framework help it to monitor and manage the security settings and controls in the digital devices.
6. **To what extent do you feel the proposed design has provided strong validation of the approach?** The proposed design has been developed to visualise and explain the proposed framework. A number of slides and a live demo of the proposed system will be presented to the participants at the beginning of the focus group session I order to provide them with a better understanding for the proposed system. Therefore, the aim of this question is to examine whether the demonstration process and simulation for the proposed design was clear and comprehensive.

7. **What do you think are the strengths in using the proposed system?** The aim of this question is to find out the opinion of the experts about the strengths of deploying the proposed model.
8. **What do you think are the weaknesses or the key barriers in using the proposed system?** The aim behind this question is to find out the weaknesses or key barriers which might the proposed framework face during the deployment from the experts' perspective.
9. **To what extent do you think that the structure of the proposed design, the layout and the format are convenient and usable?** This question aims to evaluate the usability and the convenience of the proposed interfaces from the experts' perspective**.**
10. **To what extent do you feel that the provided information and presentation are easy to understand and can attract the administrator's attention?** This question was designed to evaluate the ease of understanding the provided information and the convenience of the proposed interfaces from the experts' perspective.
11. **To what extent do you think that the enrolment process for new devices in the proposed approach is easy to use and understand?** The aim behind this question is to get the experts' opinions about the enrolment process in the proposed framework.
12. **To what extent do you think the provided information in the user's profile in the administrator's side is relevant?** The answer to this question should help to get the experts' opinion about whether the provided information in the profile is relevant or not.

13. **To what extent do you feel that the provided information and presentation in the users' profile in the user's side can attract the user's attention and recognise the current threats?** Each user will have his own profile which can contain all his managed devices. The question was designed to evaluate whether the users' profile can succeed in making the user aware of the current threats or not.
14. **Is there anything else you would like to add?** The focus group session will be ended by asking the participants if they would like to add any points or suggestions.

8.6.1.2 The End users' Focus Group

The main aim of inviting end-users in a focus group discussion is to evaluate their satisfaction with the proposed approach in terms of different aspects such as usability convenience and functionality. The end-users were recruited for the focus group discussion through the student union at the university and community centres. The following criteria have been followed in order to recruit suitable participants:

- The participants should have a good level of technical skills and deal with technologies. Therefore, novice users were excluded from being recruited for the discussion as it might be difficult for them to understand the proposed approach.
- The participants should live with their families with different digital devices and technologies in order to understand the issue that the proposed system is trying to solve. Therefore, any participants who were living alone were excluded from being invited.

Originally, 8 participants were invited to the discussion. However, 2 participants were not able to attend as they were busy at the proposed time. Table 8.4 shows a summary of the participants' background and their assigned IDs.

ID	Participants' job	Gender
B1	Accountant	Male
B2	Pharmacist	Male
B3	MSc Student in business	Male
B4	Cashier	Male
B5	MSc Student in Management	Male
B6	Shop Assistant	Male

Table 8.4: End User Participants' Background

14 open-ended qualitative questions were prepared for the end-users' group. The questions were drafted and reviewed in terms of being understandable and objective in order to achieve the aims of the focus group method:

1. **To what extent do you think the proposed design can succeed in providing better security monitoring, security management and awareness in home environments?** If the proposed framework is implemented within the home environment, can the framework help it to monitor and manage the security settings and controls in the digital devices or not.
2. **To what extent are you satisfied with the proposed design?** The aim of this question is to investigate the satisfaction of the users and their opinion about the proposed design in general.
3. **What do you think about the format and layout of the interfaces?** The answer to this question should help to evaluate the format and the layout of the interfaces.
4. **To what extent are you satisfied with the used colours?** This question aims to assess the participants' satisfaction with the colour used in the interfaces.

5. **To what extent do you think the proposed system is easy to use?** It is important to examine whether the proposed framework would be easy to use or not. This question will evaluate the ease of use of the framework.
6. **To what extent do you feel that it is easy to understand the components and features of each interface of the system?** This question was designed to evaluate how the participants find it easy to understand the components and the features of the proposed design.
7. **How do you feel about the provided information, features and sections added in the main dashboard? Relevant? Useful? Convenient?** The purpose behind this question is to investigate the participants' opinion about the relevance, the usefulness and the convenience of the information provided in the main dashboard.
8. **To what extent do you feel the main dashboard allow you to quickly identify and recognise the current threats in the managed devices?** The answer to this question should help to examine the effectiveness of the main dashboard in helping and alerting the administrator about the current threats or issues.
9. **To what extent do you think that the management interface structure and layout are convenient and usable?** The question aims to evaluate the usability and the convenience of the management interface.
10. **Does the user profile in the management interface give you the information you need about the users and the devices? If not, what is missing?** The answer to this question is to investigate whether the user profile provides the required information or not.
11. **What is your opinion about the structure, layout and the components of the user profile in the management interface? Convenient? Usable? Relevant?**

The aim of this question is to get the opinion of the participants about the user profile in the management interface in terms of the layout, structure, components, usability, convenience and relevance.

12. **To what extent do you feel the provided information in the user profile in the agent allow users to quickly identify and recognise the current threats in their personal devices?** The answer to this question should help to examine the effectiveness of the provided information in helping the users to identify the current threats or issues.
13. **What is your opinion about the structure, layout and the components of the user profile in the agent? Convenient? Usable? Relevant?** The aim of this question is to get the opinion of the participants about the user profile in the agent in terms of the layout, structure, components, usability, convenience and relevance.
14. **Would you like to suggest anything you feel is missing from the system?** The focus group session will be ended by asking the participants if they would like to add any points or suggestions which can improve the proposed framework.

8.6.1.3 Data Management and Analysis

The two focus group discussions were digitally recorded and some notes were taken during the two discussions. All the recordings were transcribed in order to facilitate the analysis processes. All the transcripts and the recordings were stored securely and the participants remained anonymous. As this research was approved by the Faculty Research Ethics Committee with no ethical issues were mentioned (See Appendix C).

A thematic analysis was chosen as a method for analysing the data collected from the focus group discussions. The same procedures and steps which have been taken in

analyzing the collected comments from the questionnaire in the previous section will be conducted to analyse the collected data from the focus group discussions.

The following two sections present the outcomes of the two focus group sessions and highlight the point of view of the end-users and experts.

8.6.2 Experts' Focus Group Feedback

The following themes and sections are identified to discuss the focus group discussion of the experts:

A. The importance of the identified research problem

The main aim of this part of the discussion was to explore and investigate the importance of the identified research problem and how it can be seen from the perspective of the experts. In general, the participants agreed that the problem which is identified by the research is very important as many online devices are being used in homes without ministering, managing and configuring them with the appropriate security controls and settings. In general, all the interviewed experts agreed that the research problem was valid and they strongly agreed that an approach needs to be proposed to mitigate the current open issue.

A1 said that the research problem was genuine and he thought that there was a noticeable gap between the statement of the problem and the current available solutions and technologies. A2 stated that the identified problem with the information security management and awareness for home users was fairly realistic and one of the most common issues. A3 supported this perspective, he considered the research problem was a very important problem and needs to be investigated and researched. P4's opinion was also on the same direction as the others, he believed that it is a valid problem and he stated

that "*if you leave the devices without good management could make them more vulnerable. The only way to manage and monitor our home devices settings and controls is to check them manually which could be difficult if we have many digital devices. So, I think this is an important problem which needs to be solved and improved*".

B. The feasibility of the proposed framework at the operational level

This question was designed to discuss and analyse the interviewed experts' feedback about the attainability, possibility and feasibility of the proposed approach and framework. In general, the majority of the experts indicated that the proposed approach and design can be possible as a workable solution in a real environment.

A1 believed that the approach is feasible but he mentioned some ethical and privacy issues which can be experienced when implementing this framework in reality. He continues by saying that users and their devices need to be monitored and some privacy and security data need to be stored and processed in the proposed approach. A2 said that the proposed approach would be very achievable and feasible to be implemented in a real environment. However, he stated that managing different platforms, operating systems, service and technologies would not be an easy task. A3 believed that the proposed framework is very viable and feasible, he stated that "*in my opinion, I don't see any major obstacles which can prevent the proposed design from being implemented in the real world*". A4's response was positive, stating that the proposed approach would be feasible to be applied in home environment. However, his concern was about user acceptance, which is how to convince home users to use this solution because they might not be interested in using it for different reasons.

C. The utilisation of the security policies in the proposed approach

The main aim behind this section is to get feedback from the interviewed experts about utilising the concept of security policies for improving information security management and awareness for home users. The experts were of the belief that the implementation of security policies in the proposed approach for home users would be a very good idea and beneficial.

A1 believed that the idea of using a number of security policies in the proposed approach is useful and effective in providing good security management for different devices, applications and platforms. He also mentioned that it is a good idea to allow the proposed system to provide novice users with a minimum level of security requirements (low level) which needs to be implemented in their devices. A2 was of the same opinion, stating that "*the security policy is already used widely in organisations and I think if it can be applied for the home users with some changes, it would be very useful and effective in managing the security settings and configurations in home devices*". A3 thought that the use of security policies in the approach is very good and it can assist in monitoring and managing security behaviour and practices of home users. He suggested that the security policy settings can be modified by the administrator for the users without providing different security levels (low, medium, high) , saying that "*I think you should have one level which can be default level for all the users. Then, if you feel that there is a user needs to be promoted and his policy needs to be modified, you can modify the policies for the user*". P4 was very positive with the utilisation of security policies in the proposed approach, saying the application of security policy is very effective in the enterprise level and it would be a good idea to be applied for home users in order to manage and monitor their security behaviour and practices.

D. The ability of the proposed approach and design in providing better security management and awareness

This question was designed to explore and investigate to what extent the proposed approach and mock-up design can be useful in improving information security management and awareness for home users. Overall, the interviewed experts agreed that the proposed framework and design can be an effective approach in providing better security monitoring, security management and awareness in home environments.

A1 stated that the proposed approach is very useful and efficient in monitoring the digital devices in homes but some efforts need to be made in order to make the solution accepted and used by home users. A2 mentioned that it does make home users aware of any possible threats which might be experienced in a usable manner. A3 believed that many advantages in security management, monitoring and awareness can be gained by implementing the proposed approach. A4 is sure that the proposed solution can help in managing and monitoring digital devices and technologies in home networks effectively, saying "*in my opinion, if the proposed tool is implemented in a real environment, it would enhance the security management and awareness for home users*".

E. The success of the proposed design in validating the approach

The section analyses feedback from the interviewed experts in order to investigate to what extent the proposed design (mockup) succeed in clarifying and validating the main aspects of the proposed approach. The experts generally agreed that the proposed design has provided a robust validation of the approach.

A1 indicated that the proposed design was beneficial enough to visualise the main concept and components of the proposed approach. He added that the provided interactions in the design made the simulation clear and useful. A2 stated that the proposed design provided a good simulation but the data used in the simulation was not real data which might be considered as a limitation of the proposed design. A3 mentioned that the simulation did

a good job, saying "*apart from the technical aspects, I think the proposed design has succeeded in showing how the system would work in the real environment by interacting with different components and sections*". A4 said that the proposed design visualized the concepts of the research very well but he would have liked to have seen more scenarios to be used with the simulation process.

F. The strengths of the proposed system

It is vital to investigate the strengths and the good aspects which can be found in the proposed approach. In general, the interview experts agreed that the proposed solution, including the framework and the design, has several elements of strength.

All the experts in complete agreement that it was a great idea when applying different security policies in the proposed approach which cover different security aspects in different operating systems and different devices in home environment. A1 said "*I think the security policies give the proposed approach the ability to manage and monitor different security controls ad aspects in different technologies, this can make the tool more effective*." In addition, most of the experts indicated that that proposed design has good usable interfaces with applying different functions and colours, especially Red and Green. A2 stated that "*I think the idea of using Red and Green is very useful to let administrators or users recognise the current issues easily*".

A3 mentioned that the centralized management would make the approach powerful because it can manage and monitor different security settings and controls in different devices owned by multiple users effectively. This was supported by A4, he thought that the centralised management makes the security management easier and more efficient. A1 and A3 mentioned that the approach is not only a management tool but also provides

home users with some tips, advice and quizzes, which can improve users' security knowledge and skills effectively.

G. The weaknesses and the key barriers in the proposed system

This section analyses feedback from the interviewed experts as regards the weaknesses of the proposed approach. The majority of the experts argued that one of the barriers in the proposed approach is how to persuade home users and family members to use the proposed approach when it is implemented in a real environment. A1 said "*In my opinion, the main barrier is how you will get people and convince them to use this system*".

Another barrier mentioned by A2 is that more work needs to be done on how the settings in different devices and operating systems will be collected and checked. He stated that he would have liked to have seen more technical explanations and discussions on how the security controls will be scanned, monitored and managed in IoT technologies which might be difficult to interact with. A3 highlighted that as the proposed approach would monitor and manage security controls home users' devices, security and privacy issues need to be considered and more works are required in order to protect confidential data for home users.

A4 argued that managing the proposed approach in a novice family who do not have any member have good IT skills would be difficult, saying "*a family member who has good knowledge and skill in IT can be nominated to manage the system. What about the families who do not have a member who has a good technology experience, who will manage the system for them*?". A1, A2 and A4 indicated that the proposed design and the interfaces might require some enhancement and improvement if this solution will be implemented in a real environment in future.

H. Thoughts on the main dashboard

This question was designed to investigate to what extent the interviewed experts feel that the designed dashboard is convenient and usable. In general, Most of the experts indicated that the main dashboard interface is usable and effective by providing the administrators with the required information.

A1 mentioned that the dashboard is designed and structured very well and the included information can easily help to recognise the current issues, saying "*yes, I think the provided information is easy to understand and help the administrator to recognise the threat easily*". A2 did not see in difficulty in understanding what is going on in the main dashboard as it is very usable and convenient. However, he mentioned that the some components of the dashboard can be enhanced and improved effectively. A3 responded by saying that the dashboard is easy to understand and its design is flexible, saying "*the sections, data, general theme can be changed in the dashboard based on the administrator's needs which can make it more usable and convenient*". A4 also was of belief that the dashboard is usable and includes all the required information which can help the administrator to make an effective decision.

I. Thoughts on the enrolment process

The main aim of this question was to analyse the experts' feedback regarding the convenience and suitability of the enrolment design and the proposed processes. Most of the interviewed experts indicated that the design and process which have been proposed for the enrolment in the proposed approach are convenient and usable.

A1 said that the idea of detecting automatically the new devices connected to the home networks is very useful and convenient and useful. A2 was very positive with the enrolment process, saying "*in my opinion, doing an automatic enrolment for the novice users and allowing the users who have at least a level of it skills to configure their policies*

is a very good idea and it will add more flexibility the system". A3's opinion was also on the same direction as others, he thought that the enrolment process implemented in the proposed approach is effective and flexible as different procedures are provided for the users based on their technical skills and knowledge. A4 was not on the same opinion of the others, indicated that the enrolment processes should be done from the administrator's side by selecting the security policies and level for the users in order to avoid any mistakes during the enrolment stage.

J. Thoughts on the management and user profile interface for the administrator

This question was designed to get feedback from the interviewed experts about the management and user profile interface in terms of the convenience and usability aspects. The experts generally provide positive feedback that the management and user profile interface is useful and effective for managing digital device by the administrators.

A1 indicated that the management is easy to use and presents all the enrolled users and their devices in a hierarchical view which can give the administrators full view in order to recognise the current issues. However, he added that the management interface does not indicate who is the administrator from the list of the home users so he suggested that the administrator profile should be highlighted with a different theme or icon in order to be easily recognized in the proposed system. A2 mentioned that the management and user profile interface is clear but he suggested that it would be a good idea to add the digital devices which are not owned by any users but they are used inside the house such as smart light and security systems. A3 and A4 had the same opinion that the provided information in the profile is relevant and useful which can make it easy for the administrator to recognise the current issues in order to make an effective decision.

K. Thoughts on the user profile interface for end users

This question was designed to get feedback from the interviewed experts about the user profile interface for end users. All the experts agreed that the end user profile is clear and convenient to be used by home users.

A1 mentioned that the aspects of the profile were designed very well. He added that it was very good idea that the profile includes some tips and advice about how to mitigate the current treats and issues in each device. A2's response was positive, stating that the red and green colour has been used in the interface effectively which can be useful for attracting the user's attention and recognise the current issues or threats. A3 indicated that the quizzes provided in the user profile were very useful to increase users' knowledge and create a competitive environment. A4 was on the same opinion of the others, he agreed that providing all the digital devices owned by one user in one profile make it more usable and convenient.

8.6.3 End Users' Focus Group Feedback

The aim of this section is to analyse the received feedback which has been collected from the focus group discussion of the end users. The following themes and section are identified to discuss the result of the focus group session for end users:

A. The ability of the proposed approach and design in providing better security management and awareness

The main aim of this part of the section was to explore and investigate to what extent the end users feels that the proposed approach can improve information security management and awareness for home users from the perspective of the end users. In general, all the end users agreed that the proposed approach and design can succeed in providing better security monitoring, security management and awareness in home environments.

B1 indicated the proposed approach can enhance security management and awareness when it is implemented in home environment, saying "*from the presentation and the demo, I think this is a better method that can be accepted and be easily used to protect the home users from the possible threats*". B2's response was positive, stating that it is a very good solution which has the ability to control all the digital devices for the whole family members. B3 and B4 indicated that the capability of the proposed approach is a viable solution for improving information security management and awareness. B5 appreciated the proposed approach and its ability to improve the current security management at homes. P6 mentioned the concept of the proposed approach can succeed in improving the current situation although the solution was visualized without using real data.

B. Users' satisfaction with the proposed approach and design

This question was designed to get feedback from the interviewed end users to investigate to what extent the end users are satisfied with the proposed approach and the mockup design. Most of the end users are satisfied with the proposed solution and design including different components, features and functions.

B1 and B2 were very satisfied with the proposed solution and the presented simulation, B2 stated "*I am more than satisfied with this solution and the design that we have seen, this proposal is absolutely can meet its targets successfully*".B3 liked the idea of the proposed approach by using security policies for managing and controlling the digital devices for home users. B4 was also satisfied with the proposed approach and design but he mentioned that more scenarios need to be added and discussed in the simulation process. B5 was very convinced that it is a very satisfactory solution and design which can be used for enhancing cyber security management and awareness for home users. B6

shared the same opinion; saying "*I personally find the proposed approach highly satisfying as it is easy to use so I am happy with it*".

C. Thoughts on the format and layout of the interfaces

The main aim of this section is to analyse the end users' feedback regarding the format and layout of the designed interfaces in the mockup design. All the interviewed end users indicated that the format and the layout which have been used in the interfaces are convenient and satisfactory.

B1 found that the layout of the interfaces was designed very well with constant format. B2's response was positive, saying "*I am highly satisfied with the format and the layout because it looks very good and very interesting*." B3 shared the same opinion, saying "*I am highly satisfied with this layout andI like the flexibility to change the layout of the interfaces with different options and information*." B4 and B5 totally agreed that the information and sections in the interfaces were structured and organised very well. B6 was on the same direction of accepting the current layout and format, saying it is a convenient layout.

D. Thoughts on the used colours

This question was designed to get feedback from the interviewed end users to investigate to what extent the end users are satisfied with colours used in the mockup design. The end users generally believed that the colours used in the proposed design are appropriate and acceptable.

All the interviewed users indicated that the use of Red and Green to highlight the risk and safety for the digital devices is very effective to recognize the current issues easily. B1 indicated that the blue colour used in the proposed design. B2 and B3 found the colours

are appropriate and convenient. B4 indicated that the idea of changing the colours is interesting, saying "*I like the idea that the user can still manage the colours of the proposed design based on your desires so well done*".B5 stated the colours used in the interfaces are suitable. B6 mentioned the use of colours is fine but he suggested that the colours in the design can be reviewed in order to be used by colour blind users.

E. The ease of use of the proposed system

This question was designed to get feedback from the interviewed end users to investigate to what extent the end users feel the proposed design easy to use. Most of the end users found the components, features and services in the proposed system seems to be easy to use.

B1 and B2 mentioned that both two parts of the system: administrator and end user's system are would be easy to understand and use without critical issues when it is implemented in the future. B3's opinion was that the effective use of icons, images and colours (red and green) make the proposed design very easy to use. B4 indicated the system is easy to use but he claimed that the proposed system might be difficult for novice users. Therefore, he suggested that tutorial videos or a guideline can be provided for the users to show them how to use the system properly. B5 and B6 believed that the system would not be difficult to be used by home users, B6 said: "*after going through the live demo with you, I think it is quite an easy tool to use*".

F. Thoughts on the main dashboard

In this section, the posed question aimed at discovering the opinions of the interviewed end users related to the main dashboard design in the proposed approach. The end users

generally indicated that the design of the main dashboard interface is convenient and usable.

B1, B2 and B3 believed that the provided information, features and components in the main dashboard are useful and beneficial for the administrator to manage the devices and the users efficiently. B1 stated "*I think the provided information in the dashboard is very good and relevant for each user and device which can help in managing devices very well*". B4 mentioned that the dashboard is very organised and the red and green colours are very useful for helping the administrators to quickly identify and recognise the current threats or problems in the managed devices. B5 liked the idea of allowing the administrator to change the structure and the data presentation in the main dashboard which would make it more convenient and flexible. B6 shared the same opinion, saying "*I feel that the dashboard provide enough relevant information and I think it is very convenient which can show the current status and issues*".

G. Thoughts on the management and user profile interface for administrators

This question was designed to get feedback from the interviewed end users to explore their opinion about the design of management and user profile interface in the proposed approach. In general, the interviewee indicated that the management interface and user profile including components, structure and layout were designed very well.

B1 and B2 indicated that the management interface is very convenient and usable as it shows the whole managed devices in the home in one interface. B3' response was positive stating "*I think it is very usable to design it in a hierarchy way and using green and red which make it more convenient*". B4 mentioned that the user profile was designed very well and it includes wide information about every single user in the home which can help the administrator to take the right security decision. B6 had the same opinion, stating "*in*

my opinion, it is very clear and easy to navigate the components. Also, I think the provided information in the profile is very relevant".

H. Thoughts on the user profile for end users

In this section, the posed question aimed at discovering the opinions of the interviewed end users related to the user profile designed to be used by home users in the proposed approach. In general, the interviewed end users agreed that the design of the user profile for home users is usable and convenient.

B1 mentioned that he is not an expert in this field he feels that the proposed design id very useful and easy for being used by home users. B2 stated the user profile have not been only designed for managing security features and controls but also for improving and increasing users' knowledge in cyber security. B3's response was positive, saying "*I think from the provided information and the red and green colour, it is easy to notice and know the current threats*". B4' opinion was also on the same direction as the others, he stated that it is very easy to find the current issues or problems from the proposed design. B5 and B6 believed that the design is structured very well with easy navigation which would make it very effective and useful when it is implemented in the future.

8.7 Summary

This chapter has proposed a framework that aims to improve security management and awareness for the home users by monitoring a variety of security controls, configurations and settings. This framework has been designed to provide the home users with bespoke awareness and knowledge based on the current needs by applying different groups of security policies. In addition, the simulation process for the proposed framework has been discussed in this chapter. The mockup design was developed in order to simulate this

framework and make it easy to understand the functionalities of the framework and how it works. Different scenarios of some user types and potential issues have been created and used in the mock-up design. In addition, this chapter has explained in detail how the mock-up design dealt with different user types, increasing knowledge and awareness.

In addition, this chapter has presented the findings of the stakeholder evaluation by the two separate groups: experts and end-users. The evaluation results have shown that the experts agreed that identified research problem is a key problem that needs to be tackled by proposing a solution. In addition, the outcomes show that the experts provide positive and encouraging feedback about the proposed framework. The expert participants agreed that the proposed approach has a great potential to be implemented for monitoring and managing the security of the digital devices for home users which can help in tackling the identified research problems and related issues. The outcomes show that the proposed framework offers a novel approach for improving security management and awareness for home users by providing a bespoke security awareness. The expert participants agreed that use of different security policies will improve security management and enhance the home users' awareness and their online behaviours.

The participants from the two groups agreed the proposed design has described and simulated the main components and functions effectively by giving an idea about how it works when it is implemented in a real environment. In addition, it can be stated that the overall feedback of the participants about the proposed interface designs was positive and good in terms of the convenience of the structure, the layout, format, usability and the provided information in each interface.

However, despite the satisfactory feedback received from the participants, some experts raised some issues that need to be taken into consideration. The privacy of users during

the process of checking security compliance should be protected all the time. In addition, a method needs to be invented and implemented that can convince home users to use the proposed system in order to provide better security management and awareness for them. Moreover, there was an issue about assigning an administrator for the family that does not have any member who has good technical skills. Another limitation is that simulated data was used in the proposed design to run the simulation mock-up design during the evaluation process.

To sum up, from the above discussion and as confirmed by many participants throughout the two focus group discussions, the proposed approach system is possible and feasible to improve the monitoring, management and awareness for home users b using the application of security policies.

Chapter Nine

Conclusions and Future Work

9 Conclusions and Future Work

9.1 Introduction

After the proposed approach was being designed, simulated and evaluated, this chapter concludes the work performed during this thesis by highlighting the key achievements and contributions of the research. This followed by discussing and summarising the limitations met during the research. Finally, several potential works and directions are identified for the future research in the chapter.

9.2 Achievements of The Research

Overall, all the objectives initially set out and stated in Chapter 1 were met and accomplished in the research, with proposing and designing a novel framework for improving the security management and awareness for home users. The achievements of the research are:

- Reviewing and investigating the current state-of-the-art and the academic literature within the information security awareness domain. The approaches and methods were analysed and reviewed in order to identify the current gap in the same domain. The literature indicated that one size fits all is the most current used approach which can be considered a problem needs to be solved.

- Identifying several security requirements and controls which need to be monitored and managed in different technologies. A novel approach is proposed to map these complex requirements in a flexible and adaptable manner by considering different technologies, services, operating systems and users.

- Designing and developing flexible usable interfaces which can improve information security management and awareness by keeping users engaged and informed about any potential security threats or issues.

- Proposing and designing a novel framework which aims at enhancing security management and awareness for home users. In addition, a mock-up design has been developed to simulate the proposed framework with different assumed scenarios in order to demonstrate and visualise the processes which might be performed in the real system.

- Conducting two separate focus group discussions in order to evaluate the entire research and the proposed framework. The first evaluation discussion was conducted with 6 end-users as the framework is proposed for home users. The second evaluation session involved 4 experts in the field of information technology and security.

9.3 Limitations of the Research

Although the objectives of the research have been achieved, a number of key limitations of the research have been identified and listed below:

1. There were a challenge and difficulty in implementing the proposed approach in a real environment due to the fact that an individual PhD researcher was conducting this research with limited timeframe and resources. Therefore, implementing the proposed framework in a real environment (an operational prototype) can provide the researcher with a better understanding of the effectiveness and the functionality of the proposed approach.

2. Avoiding end-users rejection or resistance is very important to achieve the goals of the approach once it is deployed in a real environment. As a result, an optimal approach needs to be explored and suggested which can convince home users to use and get engaged with the proposed solution.

3. Checking, monitoring and managing the security settings and controls implemented in some IoT devices need to be automated. However, it might be difficult because they are using different operating system features and some technical aspects. Therefore, more work needs to be done on how security controls and settings can be monitored and managed automatically.

9.4 Scope for Future Work

This research has advanced the field of information security management and awareness for home users. However, a number of areas are identified which can be considered for the future. First of all, an optimal solution need to be identified and proposed which can be used in the proposed framework for convincing home users to use the system. This can help in enabling home users to use the proposed solution in order to manage their digital devices effectively and mitigate their resistance or rejection for the proposed approach. In addition, a prototype system needs to be developed for the proposed framework in a real environment within the home network. This will be useful in order to understand the efficiency of the proposed approach in monitoring and managing the security controls and settings which will result in improving the security management and awareness for home users. In addition, implementing the system in a production environment will help in evaluating the system effectively and discover any limitations. Moreover, further investigation can be done to explain how some IoT devices are going to be engaged with the proposed system. Further research is required to understand how these devices can

be checked, monitored and managed based on their operating system features and specifications.

References

1. Al Abdulwahid, A., Clarke, N., Stengel, I., Furnell, S. and Reich, C. (2015) 'Security, Privacy and Usability – A Survey of Users' Perceptions and Attitudes BT - Trust, Privacy and Security in Digital Business', in Fischer-Hübner, S., Lambrinoudakis, C., and López, J. (eds). Cham: Springer International Publishing, pp. 153–168.
2. Ahmed, N., Kulsum, U., Bin Azad, M. I., Momtaz, A. S. Z., Haque, M. E. and Rahman, M. S. (2018) 'Cybersecurity awareness survey: An analysis from Bangladesh perspective', *5th IEEE Region 10 Humanitarian Technology Conference 2017, R10-HTC 2017*, 2018–Janua, pp. 788–791.
3. Aken, J. E. van (2004) 'Management Research Based on the Paradigm of the Design Sciences: The Quest for Field-Tested and Grounded Technological Rules', *Journal of Management Studies*. John Wiley & Sons, Ltd (10.1111), 41(2), pp. 219–246. Available at: https://doi.org/10.1111/j.1467-6486.2004.00430.x.
4. Alarifi, A., Tootell, H. and Hyland, P. (2012) 'A study of information security awareness and practices in Saudi Arabia', *The 2nd International Conference on Communications and Information Technology (ICCIT): Digital Information Management*, pp. 6–12.
5. ALArifi, A., Tootell, H. and Hyland, P. (2012) 'Information Security Awareness in Saudi Arabia', *CONF-IRM 2012 Proceedings*, p. 57. Available at: http://aisel.aisnet.org/confirm2012/57.
6. Aleksandrova, D. (2015) *Cyber security for small businesses*. Available at: https://www.itgovernance.co.uk/blog/cyber-security-for-small-businesses (Accessed: 25 October 2019).
7. Allwood, C. M. (2012) 'The distinction between qualitative and quantitative research methods is problematic', *Quality & Quantity*. Springer, 46(5), pp. 1417–1429.

8. Alotaibi, F., Furnell, S., Stengel, I. and Papadaki, M. (2017) 'A survey of cyber-security awareness in Saudi Arabia', *2016 11th International Conference for Internet Technology and Secured Transactions, ICITST 2016*. Infonomics Society, pp. 154–158.
9. Aloul, F. A. (2010) 'Information Security Awareness in UAE : A Survey Paper Department of Computer Science & Engineering American University of Sharjah , United Arab Emirates', *2010 International Conference for Internet Technology and Secured Transactions*. IEEE, (June), pp. 1–6.
10. Alqahtani, F. H. (2017) 'Developing an information security policy: a case study approach', *Procedia Computer Science*. Elsevier, 124, pp. 691–697.
11. Amankwa, E., Loock, M. and Kritzinger, E. (2014) 'A conceptual analysis of information security education, information security training and information security awareness definitions', *2014 9th International Conference for Internet Technology and Secured Transactions, ICITST 2014*. Infonomics Society, pp. 248–252.
12. Arachchilage, N. A. G. and Cole, M. (2011) 'Design a mobile game for home computer users to prevent from phishing attacks', *International Conference on Information Society (i-Society 2011)*, pp. 485–489.
13. Atamli, A. W. and Martin, A. (2014) 'Threat-based security analysis for the internet of things', *Proceedings - 2014 International Workshop on Secure Internet of Things, SIoT 2014*. IEEE, pp. 35–43.
14. Avison, D. and Elliot, S. (2006) 'Scoping the discipline of information systems', *Information systems: the state of the field*. John Wiley & Sons Chichester, England, pp. 3–18.
15. Bashorun, A., Worwui, A. and Parker, D. (2013) 'Information security: To determine its level of awareness in an organization', in *2013 7th International Conference on*

Application of Information and Communication Technologies. IEEE, pp. 1–5.

16. Baslyman, M. and Chiasson, S. (2016) '"smells Phishy?": An educational game about online phishing scams', *eCrime Researchers Summit, eCrime*, 2016–June, pp. 91–101.
17. Bernard, H. R. (2000) *Social Research Methods: Qualitative and Quantitative Approaches*. Sage Publications. Available at: https://books.google.co.uk/books?id=VDPftmVO5lYC.
18. Berry, C. T. and Berry, R. L. (2018) 'An initial assessment of small business risk management approaches for cyber security threats', *International Journal of Business Continuity and Risk Management*, 8(1), pp. 1–10.
19. BIK (2020) *No Title*. Available at: betterinternetforkids.eu (Accessed: 2 March 2020).
20. Bless, C. and Higson-Smith, C. (2000) *Fundamentals of Social Research Methods: An African Perspective*. Juta. Available at: https://books.google.co.uk/books?id=oi9cFSb5Oc0C.
21. Bowen, P., Hash, J. and Wilson, M. (2006) 'Sp 800-100. information security handbook: A guide for managers'. National Institute of Standards & Technology.
22. Bowling, A. (2005) 'Mode of questionnaire administration can have serious effects on data quality', *Journal of public health*. Oxford University Press, 27(3), pp. 281–291.
23. Braun, V. and Clarke, V. (2006) 'Using thematic analysis in psychology', *Qualitative research in psychology*. Taylor & Francis, 3(2), pp. 77–101.
24. Bryman, A. (2016) *Social Research Methods*. Oxford University Press. Available at: https://books.google.co.uk/books?id=N2zQCgAAQBAJ.
25. Bryman, A. and Bell, E. (2011) *Business Research Methods 3e*. OUP Oxford. Available at: https://books.google.co.uk/books?id=YnCcAQAAQBAJ.

26. Bullée, J.-W. H., Montoya, L., Pieters, W., Junger, M. and Hartel, P. H. (2015) 'The persuasion and security awareness experiment: reducing the success of social engineering attacks', *Journal of experimental criminology*. Springer, 11(1), pp. 97–115.
27. Burgoyne, J. G. and Cooper, C. L. (1975) 'Evaluation methodology', *Journal of Occupational Psychology*. Wiley Online Library, 48(1), pp. 53–62.
28. Caceres, G. R. and Teshigawara, Y. (2010) 'Security guideline tool for home users based on international standards', *Information Management & Computer Security*, 18(2), pp. 101–123.
29. Cetto, A., Netter, M. and Pernul, G. (2014) 'Friend Inspector: A Serious Game to Enhance Privacy Awareness in Social Networks', *arXiv preprint arXiv: ...*. Available at: http://arxiv.org/abs/1402.5878.
30. Chandarman, R. and Van Niekerk, B. (2017) 'Students' Cybersecurity Awareness at a Private Tertiary Educational Institution', *The African Journal of Information and Communication*, (20), pp. 133–155.
31. Chapman, D. and Smalov, L. (2004) 'On Information Security Guidelines for Small/Medium Enterprises.', in *ICEIS (3)*, pp. 3–9.
32. Chen, S. Y. and MacRedie, R. D. (2005) 'The assessment of usability of electronic shopping: A heuristic evaluation', *International Journal of Information Management*, 25(6), pp. 516–532.
33. Chiasson, S., Oorschot, P. Van and Biddle, R. (2006) 'A usability study and critique of two password managers', *15th USENIX Security ...*, (August), pp. 1–16. Available at: http://dl.acm.org/citation.cfm?id=1267336.1267337%5Cnhttp://www.usenix.org/event/sec06/tech/full_papers/chiasson/chiasson.pdf.

34. Childnet (2019) *Childnet International*. Available at: http://www.childnet.com/ (Accessed: 22 June 2019).
35. CIS (2016) *The Critical Security Controls for Effective Cyber Defense*. Available at: https://www.cisecurity.org/critical-controls/documents/CSC-MASTER-VER61-FINAL.pdf.
36. CIS (2019) *CIS Controls Version 7.1*. Available at: https://www.cisecurity.org/controls/ (Accessed: 21 October 2019).
37. Cohen, L., Manion, L. and Morrison, K. R. B. (2011) *Research Methods in Education*. Routledge (Education, Research methods). Available at: https://books.google.co.uk/books?id=p7oifuW1A6gC.
38. Collis, J. and Hussey, R. (2003) *Business Research: A practical guide for undergraduate and postgraduate students*. Palgrave Macmillan. Available at: https://books.google.co.uk/books?id=jKb3MQEACAAJ.
39. ConnectSafely.org (2019) *ConnectSafely | Online Safety*. Available at: http://www.connectsafely.org/ (Accessed: 22 November 2019).
40. Corser, G., Fink, G. A. and Bielby, J. (2017) 'Internet of Things (IoT) Security Best Practices; IEEE Internet Technology Policy Community; White Paper', *IEEE: Piscataway, NJ, USA*.
41. Coyle, J. and Williams, B. (2000) 'An exploration of the epistemological intricacies of using qualitative data to develop a quantitative measure of user views of health care', *Journal of Advanced Nursing*. Wiley Online Library, 31(5), pp. 1235–1243.
42. Cramer, D. and Howitt, D. L. (2004) *The Sage dictionary of statistics: a practical resource for students in the social sciences*. Sage.
43. Creswell, J. W. (2003) *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. SAGE Publications. Available at:

https://books.google.co.uk/books?id=nSVxmN2KWeYC.

44. Creswell, J. W. and Clark, V. L. P. (2011) *Designing and Conducting Mixed Methods Research*. SAGE Publications. Available at: https://books.google.co.uk/books?id=YcdlPWPJRBcC.
45. Crossan, F. (2003) 'Research philosophy: towards an understanding', *Nurse Researcher (through 2013)*. BMJ Publishing Group LTD, 11(1), p. 46.
46. DDCMS (2018) *Code of Practice for Consumer IoT Security*. Available at: https://www.gov.uk/government/publications/secure-by-design (Accessed: 27 October 2019).
47. Dennis, A., Jones, R., Kildare, D. and Barclay, C. (2014) 'Design Science Approach to Developing and Evaluating a National Cybersecurity Framework for Jamaica', *The Electronic Journal of Information Systems in Developing Countries*. Wiley Online Library, 62(1), pp. 1–18.
48. Denzin, N. K. and Lincoln, Y. S. (2011) *The Sage handbook of qualitative research*. Sage.
49. Department for BIS (2015) *Small businesses: what you need to know about cyber security*.
50. Department for Education (2019) *Teaching online safety in schools*. Available at: https://www.gov.uk/government/publications/teaching-online-safety-in-schools (Accessed: 2 March 2020).
51. Dillman, D. A. (2011) *Mail and Internet surveys: The tailored design method--2007 Update with new Internet, visual, and mixed-mode guide*. John Wiley & Sons.
52. Dix, A. (1998) *Human-computer Interaction*. Prentice Hall Europe (Pearson education). Available at: https://books.google.co.uk/books?id=tNxQAAAAMAAJ.
53. Dworkin, S. L. (2012) 'Sample Size Policy for Qualitative Studies Using In-Depth

Interviews', *Archives of Sexual Behavior*, 41(6), pp. 1319–1320. Available at: https://doi.org/10.1007/s10508-012-0016-6.

54. ENISA (2010) *The new users' guide: How to raise information security awareness*. Available at: https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide (Accessed: 9 October 2019).
55. Esposito, E. (2018) *Low-fidelity vs. high-fidelity prototyping*. Available at: https://www.invisionapp.com/inside-design/low-fi-vs-hi-fi-prototyping/ (Accessed: 9 March 2020).
56. EU Kids Online (2020) *EU Kids Online*. Available at: http://www.lse.ac.uk/media-and-communications/research/research-projects/eu-kids-online (Accessed: 2 March 2020).
57. Feizi, A. and Wong, C. Y. (2013) 'Usability of User Interface Styles for Learning Graphical Software Applications', *International Journal of Human Computer Interaction (IJHCI)*. Citeseer, 4(1), p. 34.
58. Fetaji, M., Loskoska, S., Fetaji, B. and Ebibi, M. (2007) 'Investigating human computer interaction issues in designing efficient virtual learning environments', in.
59. Fontenele, M. P. (2017) 'Designing a method for discovering expertise in cyber security communities: an ontological approach'. University of Reading.
60. Fricker, R. D. and Schonlau, M. (2002) 'Advantages and disadvantages of Internet research surveys: Evidence from the literature', *Field methods*. Sage Publications Sage CA: Thousand Oaks, CA, 14(4), pp. 347–367.
61. Fruth, J., Schulze, C., Rohde, M. and Dittmann, J. (2013) 'E-learning of IT security threats: A game prototype for children', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8099 LNCS, pp. 162–172.

62. Fugard, A. J. B. and Potts, H. W. W. (2015) 'Supporting thinking on sample sizes for thematic analyses: a quantitative tool', *International Journal of Social Research Methodology*. Taylor & Francis, 18(6), pp. 669–684.
63. Furman, S. M., Theofanos, M. F., Choong, Y.-Y. and Stanton, B. (2012) 'Basing Cybersecurity Training on User Perceptions', *IEEE Security & Privacy*. Los Alamitos, CA, USA: IEEE Computer Society, 10(2), pp. 40–49.
64. Furnell, S. and Clarke, N. (2012) 'Power to the people? the evolving recognition of human aspects of security', *Computers and Security*. Elsevier Ltd, 31(8), pp. 983–988. Available at: http://dx.doi.org/10.1016/j.cose.2012.08.004.
65. Furnell, S. and Moore, L. (2014) 'Security literacy: The missing link in today's online society?', *Computer Fraud and Security*. Elsevier Ltd, 2014(5), pp. 12–18. Available at: http://dx.doi.org/10.1016/S1361-3723(14)70491-9.
66. Furnell, S. and Rajendran, A. (2012) 'Understanding the influences on information security behaviour', *Computer Fraud and Security*, 2012(3), pp. 12–15.
67. Furnell, S., Tsaganidi, V. and Phippen, A. (2008) 'Security beliefs and barriers for novice Internet users', *Computers and Security*. Elsevier Ltd, 27(7–8), pp. 235–240. Available at: http://dx.doi.org/10.1016/j.cose.2008.01.001.
68. Gable, G. G. (1994) 'Integrating case study and survey research methods: an example in information systems', *European journal of information systems*. Springer, 3(2), pp. 112–126.
69. Gelo, O., Braakmann, D. and Benetka, G. (2008) 'Quantitative and qualitative research: Beyond the debate', *Integrative psychological and behavioral science*. Springer, 42(3), pp. 266–290.
70. Get Safe Online (2011) *The Rough Guide to Online Safety*. Available at: www.roughguides.comwww.getsafeonline.org (Accessed: 27 October 2019).

71. GetSafeOnline.org (2019) *Get Safe Online | Free online security advice*. Available at: https://www.getsafeonline.org/ (Accessed: 22 November 2019).
72. Giannakas, F., Kambourakis, G. and Gritzalis, S. (2015) 'CyberAware: A mobile game-based app for cybersecurity education and awareness', *2015 International Conference on Interactive Mobile Communication Technologies and Learning (IMCL)*, (November), pp. 54–58. Available at: http://www.scopus.com/inward/record.url?eid=2-s2.0-84962385368&partnerID=tZOtx3y1.
73. Google (2018) *How many connected devices do you currently use?*, *Statista. Statista Inc*. Available at: https://www.statista.com/statistics/365104/number-connected-devices-per-person-uk (Accessed: 9 October 2019).
74. Google (2019) *Google Safety Centre*. Available at: https://www.google.co.uk/intl/en/safetycenter/ (Accessed: 22 August 2019).
75. Gregor, S. and Hevner, A. R. (2013) 'Positioning and presenting design science research for maximum impact', *MIS quarterly*. JSTOR, pp. 337–355.
76. Guba, E. G. and Lincoln, Y. S. (1994) 'Competing paradigms in qualitative research', *Handbook of qualitative research*. Sage, Thousand Oaks, CA, 2(163–194), p. 105.
77. Guest, G., Bunce, A. and Johnson, L. (2006) 'How many interviews are enough? An experiment with data saturation and variability', *Field methods*. Sage Publications Sage CA: Thousand Oaks, CA, 18(1), pp. 59–82.
78. Gupta, A. and Hammond, R. (2005) 'Information systems security issues and decisions for small businesses: An empirical examination', *Information Management and Computer Security*, 13(4), pp. 297–310.
79. Haeussinger, F. and Kranz, J. (2013) 'Information security awareness: Its antecedents and mediating effects on security compliant behavior'.

80. Hale, M. L., Gamble, R. F. and Gamble, P. (2015) 'CyberPhishing: A game-based platform for phishing awareness testing', *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2015–March, pp. 5260–5269.
81. Hammel, E. A. and Laslett, P. (1974) 'Comparing household structure over time and between cultures', *Comparative studies in society and history*. Cambridge University Press, 16(1), pp. 73–109.
82. Harris, J. (2011) 'Techniques for managing strategic partnership working arrangements in local government'. University of Reading.
83. Henderson, K. A. (2011) 'Post-positivism and the pragmatics of leisure research', *Leisure Sciences*. Taylor & Francis, 33(4), pp. 341–346.
84. Herley, C. (2009) 'So long, and no thanks for the externalities: The rational rejection of security advice by users', in *Proceedings New Security Paradigms Workshop*, pp. 133–144.
85. Hevner, A. ., March, S. T., Park, J. and Ram, S. (2004) 'Design science in information systems research', *MIS quarterly*. Springer, 28(1), pp. 75–105.
86. Hevner, A. and Chatterjee, S. (2010) *Design research in information systems: theory and practice*. Springer Science & Business Media.
87. Hewett, T. T. *et al.* (1992) *ACM SIGCHI curricula for human-computer interaction*. ACM.
88. Hinkle, D. E., Wiersma, W. and Jurs, S. G. (2003) *Applied Statistics for the Behavioral Sciences*. Houghton Mifflin (Applied Statistics for the Behavioral Sciences). Available at: https://books.google.co.uk/books?id=7tntAAAAMAAJ.
89. Howe, A. E., Ray, I., Roberts, M., Urbanska, M. and Byrne, Z. (2012) 'The Psychology of Security for the Home Computer User', in *2012 IEEE Symposium on Security and Privacy*. San Francisco, pp. 209–223.

90. Huang, K.-Y. (2009) ‘Challenges in human-computer interaction design for mobile devices’, in *Proceedings of the World Congress on Engineering and Computer Science*. San Francisco, USA, pp. 236–241.
91. IBA (2018) *Cybersecurity Guidelines Cyber Security Guidelines By the IBA’s Presidential Task Force on Cyber Security*. Available at: https://www.ibanet.org/LPRU/cybersecurity-guidelines.aspx (Accessed: 27 October 2019).
92. Ibrahim, T., Furnell, S. M., Papadaki, M. and Clarke, N. L. (2010) ‘Assessing the usability of end-user security software’, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 6264 LNCS, pp. 177–189.
93. Iivari, J. and Venable, J. (2009) ‘Action research and design science research - Seemingly similar but decisively dissimilar’, *17th European Conference on Information Systems, ECIS 2009*, (June 2014).
94. Iivari, J. and Venable, J. R. (2009) ‘Action research and design science research-seemingly similar but decisively dissimilar’.
95. In, J. (2017) ‘Introduction of a pilot study’, *Korean journal of anesthesiology*. 2017/11/14. The Korean Society of Anesthesiologists, 70(6), pp. 601–605. Available at: https://www.ncbi.nlm.nih.gov/pubmed/29225742.
96. Information Commissioner’s Office (2016) *A practical guide to IT security Ideal for the small business*.
97. International Organization for Standardization (ISO) (2013) *ISO/IEC27002: 2013 Information technology—Code of practice for information security controls*, *Iec*.
98. Internetmatters.org (2019) *Information, Advice and Support to Keep Children Safe Online*. Available at: https://www.internetmatters.org/ (Accessed: 22 October 2019).

99. ITU (2007) *ITU-T Recommendation X.1111: Framework of security technologies for home network*, *International Telecommunication Union*. Available at: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1111-200702-I!!PDF-E&type=items.

100. ITU (2018) *Number of internet users worldwide from 2005 to 2018 (in millions)*. Available at: https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/ (Accessed: 16 August 2019).

101. Jahankhani, H., Jayaraveendran, T. and Kapuku-Bwabw, W. (2011) 'Improved awareness on fake websites and detecting techniques', in *Global Security, Safety and Sustainability & e-Democracy*. Berlin, Heidelberg: Springer, pp. 271–279.

102. Johnson, B. and Turner, L. A. (2003) 'Data collection strategies in mixed methods research', *Handbook of mixed methods in social and behavioral research*, pp. 297–319.

103. Johnson, R. B. and Onwuegbuzie, A. J. (2004) 'Mixed methods research: A research paradigm whose time has come', *Educational researcher*. Sage Publications Sage CA: Thousand Oaks, CA, 33(7), pp. 14–26.

104. Johnston, J., Eloff, J. H. P. and Labuschagne, L. (2003) 'Security and human computer interfaces', *Computers and Security*, 22(8), pp. 675–684.

105. Juhari, S. F. and Zin, N. A. M. (2013) 'No Educating Children about Internet Safety through Digital Game Based Learning', *International Journal of Interactive Digital Media*, 1(1), pp. 65–70.

106. Kagioglou, M., Cooper, R., Aouad, R., Hinks, J., Sexton, M. and Sheath, D. (1998) *A Generic Guide to the Design and Construction Process Protocol*. The University of Salford.

107. Kamariza, Y. (2017) 'Implementation of information security policies in public

organizations : Top management as a success factor', (May). Available at: http://www.diva-portal.org/smash/get/diva2:1154975/FULLTEXT01.pdf [Accessed 29 May 2018].

108. Kappen, D. L. (2019) *Simplifying Design Science Research, Action Research and Design Research*. Available at: https://medium.com/@3D_Ideation/simplifying-design-science-research-action-research-and-design-research-bf564959402b (Accessed: 8 March 2020).

109. Karavaras, E., Magkos, E. and Tsohou, A. (2016) 'Low User Awareness Against Social Malware: An Empirical Study and Design of a Security Awareness Application', *13th European Mediterranean & Middle Eastern Conference on Information Systems (EMCIS 2016)*, pp. 1–10.

110. Katadae, A. (2000) *Phenomenological Understanding of the Meaning in Lifeworld: Bridging Philosophy and Research Methodology*.

111. Katsabas, D., Furnell, S. and Dowland, P. (2005) 'Using Human Computer Interaction principles to promote usable security', *Proceedings of the Fifth International Network Conference (INC 2005)*, pp. 5–7. Available at: http://ro.ecu.edu.au/ecuworks/2726/.

112. Kaur, J. and Mustafa, N. (2013) 'Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME', in *International Conference on Research and Innovation in Information Systems, ICRIIS*. IEEE, pp. 286–290.

113. Keller, S., Powell, A., Horstmann, B., Predmore, C. and Crawford, M. (2005) 'Information security threats and practices in small businesses', *Information Systems Management*, 22(2), pp. 7–19.

114. Kendall, K. E. and Kendall, J. E. (2010) *Systems analysis and design*. Prentice

Hall Press.

115. Knapp, K. J., Morris, R. F., Marshall, T. E. and Anthony, T. (2009) 'Information security policy : An organizational-level process model', *Computers & Security*. Elsevier Ltd, 28(7), pp. 493–508. Available at: http://dx.doi.org/10.1016/j.cose.2009.07.001.

116. Kritzinger, E. and Von Solms, S. H. (2010) 'Cyber security for home users: A new way of protection through awareness enforcement', *Computers and Security*. Elsevier Ltd, 29(8), pp. 840–847. Available at: http://dx.doi.org/10.1016/j.cose.2010.08.001.

117. Kritzinger, E. and Von Solms, S. H. (2013) 'Home User Security- from Thick Security-oriented Home Users to Thin Security- oriented Home Users', *Science and Information Conference (SAI), 2013*, pp. 340–345. Available at: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6661760.

118. Krueger, R. A. (1997) *Developing questions for focus groups*. Sage Publications.

119. Krueger, R. A. and Casey, M. A. (2014) *Focus groups: A practical guide for applied research*. Sage publications.

120. Kuechler, W. and Vaishnavi, V. (2012) 'A framework for theory development in design science research: multiple perspectives', *Journal of the Association for Information systems*. Citeseer, 13(6), p. 395.

121. Labuschagne, W. A., Burke, I., Veerasamy, N. and Eloff, M. M. (2011) 'Design of cyber security awareness game utilizing a social media framework', *2011 Information Security for South Africa - Proceedings of the ISSA 2011 Conference*.

122. Labuschagne, W. A. and Eloff, M. (2012) 'Towards an automated security awareness system in a virtualized environment', in *11th European Conference on Information Warfare and Security 2012, ECIW 2012*, pp. 163–171.

123. Lazarinis, F., Alexandri, K., Verykios, V. S. and Panagiotakopoulos, C. (2015) 'Raising safer internet awareness through a mobile application based on contrasting visual stories', *Interactive Mobile Communication Technologies and Learning (IMCL), 2015 International Conference on*, pp. 88–90.

124. Lee, A. S. (1991) 'Integrating positivist and interpretive approaches to organizational research', *Organization science*. INFORMS, 2(4), pp. 342–365.

125. Lehaney, B. A. and Vinten, G. (1994) '"Methodology": An Analysis of Its Meaning and Use', *Work study*. MCB UP Ltd, 43(3), pp. 5–8.

126. Lejaka, T. K., Da Veiga, A. and Loock, M. (2019) 'Cyber security awareness for small, medium and micro enterprises (SMMEs) in South Africa', *2019 Conference on Information Communications Technology and Society, ICTAS 2019*, pp. 1–6.

127. Leon, A. C., Davis, L. L. and Kraemer, H. C. (2011) 'The role and interpretation of pilot studies in clinical research', *Journal of psychiatric research*. 2010/10/28, 45(5), pp. 626–629. Available at: https://www.ncbi.nlm.nih.gov/pubmed/21035130.

128. Lincoln, Y. S., Guba, E. G. and Publishing, S. (1985) *Naturalistic Inquiry*. SAGE Publications. Available at: https://books.google.co.uk/books?id=2oA9aWlNeooC.

129. Liyanage, E. (2016) *10 Usability heuristics explained*. Available at: https://medium.com/@erangatl/10-usability-heuristics-explained-caa5903faba2 (Accessed: 7 October 2019).

130. Lunsford, P. and Boahn, C. (2015) *How the Lizard Squad Took Down Two of the Biggest Networks in the World*. Available at: https://infosecwriters.com/Papers/JRollins_Lizard_Squad.pdf (Accessed: 1 March 2019).

131. Maayan, G. (2020) *The IoT Rundown For 2020: Stats, Risks, and Solutions*. Available at: https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-

2020.aspx?Page=1 (Accessed: 4 April 2020).

132. Magaya, R. T. and Clarke, N. L. (2012) 'Web-based risk analysis for home users', in *10th Australian Information Security Management Conference, AISM 2012*, pp. 19–27.

133. Mahjabin, T., Xiao, Y., Sun, G. and Jiang, W. (2017) 'A survey of distributed denial-of-service attack, prevention, and mitigation techniques', *International Journal of Distributed Sensor Networks*, 13(12).

134. Malhotra, N. K., Peterson, M. and Kleiser, S. B. (1999) 'Marketing research: A state-of-the-art review and directions for the twenty-first century', *Journal of the academy of marketing science*. Sage Publications Sage CA: Thousand Oaks, CA, 27(2), pp. 160–183.

135. Mallett, S. (2004) 'Understanding home: a critical review of the literature', *The sociological review*. SAGE Publications Sage UK: London, England, 52(1), pp. 62–89.

136. Maurer, M., Luca, A. De and Kempe, S. (2011) 'Using Data Type Based Security Alert Dialogs to Raise Online Security Awareness', *SOUPS '11 Proceedings of the Seventh Symposium on Usable Privacy and Security*, p. Paper 2.

137. Microsoft (2019) *Online Safety - YouthSpark Hub*. Available at: https://www.microsoft.com/about/philanthropies/youthspark/youthsparkhub/programs/onlinesafety/ (Accessed: 22 January 2019).

138. Mingers, J. (2004) 'Re-establishing the real: critical realism and information systems', *Social theory and philosophy for information systems*. New York: Wiley, 372(1).

139. Mingers, J., Mutch, A. and Willcocks, L. (2013) 'Critical realism in information systems research', *MIS quarterly*. JSTOR, 37(3), pp. 795–802.

140. Mingers, J. and Willcocks, L. (2014) 'An integrative semiotic framework for information systems: The social, personal and material worlds', *Information and Organization*. Elsevier, 24(1), pp. 48–70.

141. Morgan, D. L. (1996) 'Focus groups', *Annual review of sociology*. Annual Reviews 4139 El Camino Way, PO Box 10139, Palo Alto, CA 94303-0139, USA, 22(1), pp. 129–152.

142. Morgan, R. (2006) 'Information security in small businesses'.

143. Morse, J. M. and Chung, S. E. (2003) 'Toward holism: The significance of methodological pluralism', *International Journal of Qualitative Methods*. SAGE Publications Sage CA: Los Angeles, CA, 2(3), pp. 13–20.

144. Muller, M. (Microsoft), Matheson, L. (Microsoft), Page, C. (Microsoft) and Gallup, R. (Microsoft) (1998) 'Participatory Heuristic Evaluation', *Interactions*, (october), pp. 13–18.

145. Muñoz-Arteaga, J., González, R. M., Martin, M. V., Vanderdonckt, J. and Álvarez-Rodríguez, F. (2009) 'A methodology for designing information security feedback based on User Interface Patterns', *Advances in Engineering Software*. Elsevier, 40(12), pp. 1231–1241.

146. Myers, B. (1994) 'Challenges of HCI design and implementation', *interactions*. ACM, 1(1), pp. 73–83.

147. Myers, M. D. (1997) 'Qualitative research in information systems', *MIS Quarterly*. Society for Information Management and The Management Information Systems …, 21(2), pp. 241–242.

148. Narayana Samy, G., Ahmad, R. and Ismail, Z. (2010) 'Security threats categories in healthcare information systems', *Health informatics journal*. SAGE Publications Sage UK: London, England, 16(3), pp. 201–209.

149. National Office of Statisitcs (2018) *Internet access - households and individuals, Great Britain: 2018*. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2018 (Accessed: 2 March 2019).

150. NCSA and McAfee (2011) *2011 NCSA / McAfee Internet Home Users Survey*. Available at: https://staysafeonline.org/download/datasets/2068/NCSA_McAfee_Online User Study_Final_11_15_11.pdf (Accessed: 22 June 2017).

151. NCSA and McAfee (2012) *2012 NCSA / McAfee Online Safety Survey*. Available at: https://staysafeonline.org/download/datasets/3890/2012_ncsa_mcafee_online_safety_study.pdf (Accessed: 22 June 2017).

152. NCSA and PayPal (2013) *2013 NATIONAL ONLINE SAFETY STUDY*. Available at: https://staysafeonline.org/download/datasets/7358/2013 NCSA Online Safety Study.pdf (Accessed: 22 June 2017).

153. NCSC (2018a) *10 steps to cyber security - NCSC*. Available at: https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps (Accessed: 25 October 2019).

154. NCSC (2018b) *Password administration for system owners*. Available at: https://www.ncsc.gov.uk/collection/passwords?curPage=/collection/passwords/updating-your-approach (Accessed: 26 February 2020).

155. Neuman, W. L. (2000) *Social Research Methods: Qualitative and Quantitative Approaches*. Allyn and Bacon (Fifth ed). Available at: https://books.google.co.uk/books?id=d7PpAAAAIAAJ.

156. Newbould, M. . and Furnell, S. (2009) 'Playing Safe: A prototype game for raising awareness of social engineering', *Australian Information Security Management …*, (December), pp. 24–30. Available at: http://www.scopus.com/inward/record.url?eid=2-s2.0-84864552106&partnerID=40&md5=c35c02b54b3c5929bc9cdb6fffd4c843%5Cnhttp://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1003&context=ism.

157. Ng, B. B.-Y. and Rahim, M. A. (2005) 'A Socio-Behavioral Study of Home Computer Users ' Intention to Practice Security', *Proceedings of the Ninth Pacific Asia Conference on Information Systems*, 2003, pp. 234–247. Available at: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1132&context=pacis2005.

158. Nielsen, J. (1994) *10 Usability Heuristics for User Interface Design*. Available at: https://www.nngroup.com/articles/ten-usability-heuristics/ (Accessed: 7 May 2019).

159. NIST (2014) 'Security and Privacy Controls for Federal Information Systems and Organizations Security and Privacy Controls for Federal Information Systems and Organizations', *Sp-800-53Ar4*, p. 400+.

160. NIST (2019) *NIST Publications*. Available at: https://csrc.nist.gov/publications (Accessed: 21 October 2019).

161. Norton (2016) *Norton Security Center, A Complete Online Security Resource*. Available at: https://us.norton.com/security-center/ (Accessed: 22 December 2016).

162. NSA (2016) *Best Practices for Keeping Your Home Network Secure*. Available at: https://www.dni.gov/files/NCSC/documents/campaign/NSA-guide-Keeping-Home-Network-Secure.pdf (Accessed: 14 October 2019).

163. Nthala, N., Flechais, I., Nthala, N. and Flechais, I. (2018) 'Informal Support Networks : an investigation into Home Data Security Practices', *In Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*, pp. 63–82.

164. Nykänen, R. and Kärkkäinen, T. (2018) 'A Knowledge Interface System for Information and Cyber Security Using Semantic Wiki', in *International Conference on Design Science Research in Information Systems and Technology*. Springer, pp. 316–330.

165. Obied, A. and Alhajj, R. (2009) 'Fraudulent and malicious sites on the web', *Applied intelligence*. Springer, 30(2), pp. 112–120.

166. Ofcom (2015) *Adults' media use and attitudes*. Available at: http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/media-lit-10years/2015_Adults_media_use_and_attitudes_report.pdf (Accessed: 25 June 2017).

167. Ofcom (2018) *Adults' media use and attitudes report*. Available at: http://stakeholders.ofcom.org.uk/market-data-research/media-literacy/media-lit-research/adults-2013/ (Accessed: 1 March 2019).

168. Ofcom (2019) *Adults' media use and attitudes report*. Available at: http://stakeholders.ofcom.org.uk/market-data-research/media-literacy/media-lit-research/adults-2013/.

169. Onwubiko, C. and Lenaghan, A. P. (2007) 'Managing security threats and vulnerabilities for small to medium enterprises', in *2007 IEEE Intelligence and Security Informatics*. IEEE, pp. 244–249.

170. Ophoff, J. and Robinson, M. (2014) 'Exploring end-user smartphone security awareness within a South African context', *2014 Information Security for South Africa - Proceedings of the ISSA 2014 Conference*. IEEE, pp. 1–7.

171. Orlikowski, W. J. and Baroudi, J. J. (1991) 'Studying information technology in organizations: Research approaches and assumptions', *Information systems research*. INFORMS, 2(1), pp. 1–28.

172. Osborn, E. and Simpson, A. (2015) 'Small-Scale Cyber Security', in *Proceedings - 2nd IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2015 - IEEE International Symposium of Smart Cloud, IEEE SSC 2015*. IEEE, pp. 247–252.

173. Osborn, E. and Simpson, A. (2017) 'On small-scale IT users' system architectures and cyber security: A UK case study', *Computers and Security*. Elsevier Ltd, 70, pp. 27–50. Available at: https://doi.org/10.1016/j.cose.2017.05.001.

174. Ousmanou, K. (2007) 'A Method for the Articulation of Users' Requirements for Personalised Information Provision'. University of Reading.

175. Parker, B. (1998) *Globalization and business practice: managing across boundaries*. Sage Publications. Available at: https://books.google.co.uk/books?id=EiW1AAAAIAAJ.

176. Peltier, T. R. (2016) *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. Auerbach Publications.

177. Potgieter, M., Marais, C. and Gerber, M. (2013) 'Fostering Content Relevant Information Security Awareness through Browser Extensions', in *IFIP World Conference on Information Security Education*. Berlin, Heidelberg: Springer, pp. 58–67.

178. Price, I. (2000) 'Research Methods and Statistics. PESS202, Lecture and Commentary Notes', *University of New England, Armidale*.

179. Proença, D. and Borbinha, J. (2018) 'Information security management systems-a maturity model based on ISO/IEC 27001', in *International Conference on Business Information Systems*. Springer, pp. 102–114.

180. Quartey, P. (2003) 'Finance and Small and Medium-sized Enterprise development in Ghana'. University of Manchester.

181. Rajasekar, S., Philominathan, P. and Chinnathambi, V. (2013) 'Research Methodology. Available from arxiv. org/pdf', *arXiv preprint physics/0601009*.

182. Rani, C. and Goel, S. (2015) 'CSAAES: An expert system for cyber security attack awareness', *International Conference on Computing, Communication and Automation, ICCCA 2015*, pp. 242–245.

183. Rao, U. H. and Pati, B. P. (2012) 'Study of internet security threats among home users', in *2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN)*. Sao Carlos, pp. 217–221. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6412405.

184. Rapoport, R. N. (1970) 'Three dilemmas in action research: with special reference to the Tavistock experience', *Human relations*. Sage Publications Sage CA: Thousand Oaks, CA, 23(6), pp. 499–513.

185. Reid, R. and Van Niekerk, J. (2014) 'Snakes and ladders for digital natives: information security education for the youth', *Information Management & Computer Security*, 22(2), p. 179. Available at: http://search.proquest.com/docview/1660152864?accountid=10610%5Cnhttp://sfxhosted.exlibrisgroup.com/duquesne?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&genre=article&sid=ProQ:ProQ:abiglobal&atitle=Snakes+and+ladders+for+digital+natives:

186. Reubens, R. (2016) 'To craft, by design, for sustainability: Towards holistic sustainability design for developing-country enterprises'.

187. Reynolds, M. (2016) *TalkTalk and Post Office customers hit by Mirai worm attack*. Available at: https://www.wired.co.uk/article/deutsche-telekom-cyber-attack-mirai (Accessed: 19 March 2019).

188. Ritchie, J., Lewis, J., Nicholls, C. M. and Ormston, R. (2013) *Qualitative research*

practice: A guide for social science students and researchers. sage.

189. Robson, C. (2002) *Real World Research: A Resource for Social Scientists and Practitioner-Researchers*. Wiley (Regional Surveys of the World Series). Available at: https://books.google.co.uk/books?id=DkplMcAysFQC.

190. Runeson, P., Host, M., Rainer, A. and Regnell, B. (2012) *Case study research in software engineering: Guidelines and examples*. John Wiley & Sons.

191. Safa, N. S., Von Solms, R. and Furnell, S. (2016) 'Information security policy compliance model in organizations', *computers & security*. Elsevier, 56, pp. 70–82.

192. SafeandSecureOnline.org (2019) *Safe and Secure Online by ISC2*. Available at: https://safeandsecureonline.org/ (Accessed: 22 July 2019).

193. Saferinternet.org.uk (2019) *UK Safer Internet Centre*. Available at: http://www.saferinternet.org.uk/ (Accessed: 23 June 2019).

194. Sangani, N. K. and Vijayakumar, B. (2012) 'Cyber security scenarios and control for small and medium enterprises', *Informatica Economica*. Citeseer, 16(2), p. 58.

195. SANS (2014) *SANS Renews Library of Information Security Policy Templates | SANS Institute: Press*. Available at: https://www.sans.org/press/announcement/2014/09/03/2 (Accessed: 21 October 2019).

196. Saunders, M., Lewis, P. and Thornhill, A. (2009) *Research Methods for Business Students*. Prentice Hall (Always learning). Available at: https://books.google.co.uk/books?id=u-txtfaCFiEC.

197. Saunders, P. and Williams, P. (1988) 'The constitution of the home: towards a research agenda', *Housing studies*. Taylor & Francis, 3(2), pp. 81–93.

198. Scholtz, J., Muller, M., Novick, D., Olsen Jr, D. R., Shneiderman, B. and Wharton, C. (1999) 'A research agenda for highly effective human-computer interaction:

useful, usable, and universal', *ACM SIGCHI Bulletin*. ACM, 31(4), pp. 13–16.

199. Serrhini, M. and Moussa, A. A. (2013) 'Home users security and the web browser inbuilt settings, framework to setup it automatically', *Journal of Computer Science*, 9(2), pp. 159–168.

200. Sharifi, M., Fink, E. and Carbonell, J. G. (2011) 'SmartNotes: Application of crowdsourcing to the detection of web threats', *Conference Proceedings - IEEE International Conference on Systems, Man and Cybernetics*, pp. 1346–1350.

201. Sherif, E., Furnell, S. and Clarke, N. (2015) 'Awareness, behaviour and culture: The ABC in cultivating security compliance', in *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE, pp. 90–94.

202. Shneiderman, B. and Plaisant, C. (2004) *Designing the User Interface: Strategies for Effective Human-Computer Interaction (4th Edition)*. Pearson Addison Wesley.

203. Shostack, A. (2014) *Threat Modeling: Designing for Security*. Wiley. Available at: https://books.google.co.uk/books?id=asPDAgAAQBAJ.

204. Silver, C. and Lewins, A. (2014) *Using software in qualitative research: A step-by-step guide*. Sage.

205. Smith, A., Papadaki, M. and Furnell, S. M. (2013) 'Improving awareness of social engineering attacks', *IFIP Advances in Information and Communication Technology*, 406, pp. 249–256.

206. Von Solms, B. (2015) 'Improving South Africa's Cyber Security by cyber securing its small companies', *2015 IST-Africa Conference, IST-Africa 2015*. IIMC International Information Management Corporation Ltd., pp. 1–8.

207. StaySafeOnline.org (2018) *National Cyber Security Alliance | StaySafeOnline.org*. Available at: https://staysafeonline.org/ (Accessed: 22 November 2019).

208. Susman, G. I. (1983) 'Action research: a sociotechnical systems perspective', *Beyond method: Strategies for social research*. Sage Beverly Hills, CA, 95, p. 113.

209. Symantec (2019) *Internet Security Threat Report*. Available at: https://img03.en25.com/Web/Symantec/%7Bdfc1cc41-2049-4a71-8bd8-12141bea65fd%7D_ISTR_24_2019_en.pdf.

210. Talib, S., Clarke, N. L. and Furnell, S. M. (2010) 'An analysis of information security awareness within home and work environments', *ARES 2010 - 5th International Conference on Availability, Reliability, and Security*. IEEE, pp. 196–203.

211. Taylo, H. (2015) *Biggest cybersecurity threats in 2016*.

212. Teijlingen, E. R. and Hundley, V. (2001) 'The importance of pilot studies'. Department of Sociology, University of Surrey.

213. Teymourlouei, H. (2015) 'Quick Reference : Cyber Attacks Awareness and Prevention Method for Home Users', *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, 9(3), pp. 480–486. Available at: http://www.waset.org/publications/10000665.

214. Thomas, K. (2001) *Building a Secure Home Network*, *SANS Institute*.

215. Tipton, H. F. and Nozaki, M. K. (2007) *Information security management handbook*. CRC press.

216. Titchen, A. and Hobson, D. (2005) 'Phenomenology', *Research methods in the social sciences*, pp. 121–130.

217. Tolnai, A. and Von Solms, S. (2009) 'Solving security issues using information security awareness portal', *2009 International Conference for Internet Technology and Secured Transactions, (ICITST)*, pp. 1–5.

218. Toomela, A. (2008) 'Variables in psychology: A critique of quantitative

psychology', *Integrative Psychological and Behavioral Science*. Springer, 42(3), pp. 245–265.

219. Toth, P. R. and Paulsen, C. (2016) *Small Business Information Security: The Fundamentals*.

220. US-CERT (2001) *Home Network Security*. Available at: https://www.us-cert.gov/Home-Network-Security#history (Accessed: 14 October 2019).

221. US-CERT (2015) *Security Tip (ST15-002): Home Network Security*, *NCCIC Publications*. Available at: https://www.us-cert.gov/ncas/tips/ST15-002 (Accessed: 14 October 2019).

222. Vaishnavi, V. K. and Kuechler, W. (2007) 'Design Science Research Methods and Patterns: Innovating Information and Communication Technology'. Auerbach Publications.

223. Da Veiga, A. and Eloff, J. H. P. (2010) 'A framework and assessment instrument for information security culture', *Computers & Security*. Elsevier, 29(2), pp. 196–207.

224. Volkamer, M., Renaud, K., Canova, G., Reinheimer, B. and Braun, K. (2015) 'Design and Field Evaluation of PassSec: Raising and Sustaining Web Surfer Risk Awareness', in *International Conference on Trust and Trustworthy Computing, TRUST 2015,*. Cham: Springer, pp. 104–122.

225. W Creswell, J. (2016) 'Research Design.: Qualitative, Quantitative, Mixed Methods Approaches'. University Of Nebraska-Lincoln.

226. Wash, R. and Rader, E. (2011) 'Influencing mental models of security', *Proceedings of the 2011 workshop on New security paradigms workshop - NSPW '11*, pp. 57–67. Available at: http://dl.acm.org/citation.cfm?doid=2073276.2073283.

227. Watson, B. and Zheng, J. (2017) 'On the User Awareness of Mobile Security

Recommendations', *Proceedings of the SouthEast Conference*, (ACM), pp. 120–127.

228. Weber, S. (2010) 'Design science research: Paradigm or approach?', in *AMCIS*, p. 214.

229. Webwise (2019) *Webwise | The Irish Internet Safety Awareness Centre*. Available at: https://www.webwise.ie/ (Accessed: 22 October 2019).

230. Whitman, M. E. and Mattord, H. J. (2016) *Management of Information Security*. Cengage Learning. Available at: https://books.google.co.uk/books?id=bKMZDAAAQBAJ.

231. Whitten, A. and Tygar, J. D. (1999) 'Why Johnny can't encrypt: A usability evaluation of PGP 5.0', *Proceedings of the 8th USENIX Security Symposium*, (August), pp. 169–184. Available at: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Why+Johnny+can?t+encrypt:+A+usability+evaluation+of+PGP+5.0#0.

232. Wilson, M. and Hash, J. (2003) 'Building an information technology security awareness and training program', *NIST Special publication*, 800(50), pp. 1–39.

233. Wilson, M., de Zafra, D. E., Pitcher, S. I., Tressler, J. D. and Ippolito, J. B. (1998) *Information technology security training requirements: A role-and performance-based model*. NATIONAL INST OF STANDARDS AND TECHNOLOGY GAITHERSBURG MD COMPUTER SECURITY DIV.

234. Wiredsafety (2019) *wired safety*. Available at: http://www.wiredsafety.com/ (Accessed: 22 December 2016).

235. Woody, C. and Clinton, L. (2004) 'Common Sense Guide to Cyber Security for Small Businesses, Recommended Actions for Information Security'. Carnegie Mellon University and Internet Security Alliance.

236. Yang, C. C., Tseng, S. S., Lee, T. J., Weng, J. F. and Chen, K. (2012) 'Building

an anti-phishing game to enhance network security literacy learning', *Proceedings of the 12th IEEE International Conference on Advanced Learning Technologies, ICALT 2012*, pp. 121–123.

237. Zimmerman, J., Forlizzi, J. and Evenson, S. (2007) 'Research through design as a method for interaction design research in HCI', *Conference on Human Factors in Computing Systems - Proceedings*, pp. 493–502.

Appendix A: A User Survey

I am am a PhD candidate at the University of Plymouth in the School of Computing. I am conducting this survey as part of my PhD research project. The purpose of this survey is to explore the cyber security knowledge, awareness and concerns among the home users. In addition, it will investigate the possibility of developing a system which can manage the security digital devices for home users. Moreover, several initial interfaces will be evaluated by the participants in terms of the usability and the functionality.

As a participant, you are invited to participate in this questionnaire which will require approximately 15 minutes to complete. The result of data which will be collected from your participation will provide useful information which will assist the researchers to accomplish the main goals of the research.

At all stages of the study, your responses will remain anonymous since no personal information or IP addresses will be collected. In addition, your participation will remain confidential and no one will be able to identify you or your answers. Therefore, there is no risk for taking this survey.

You have the right to withdraw at any stage upon until the completion of the survey. However, the data collected from your participation cannot be removed as we are not able to identify your answers.

Your participation is voluntary. If you wish to take part, you will need to agree for participating by clicking the button below. You may withdraw at any time during the survey.

For information regarding the study, please contact: Fayez Alotaibi – fayez.alotaibi@plymouth.ac.uk

For any questions concerning the ethical status of this study, please contact the secretary of the Human Ethics Committee – paula.simson@plymouth.ac.uk

Fayez Alotaibi

PhD Researcher

The University of Plymouth

fayez.alotaibi@plymouth.ac.uk

○ I consent, begin the study

○ I do not consent, I do not wish to participate

Skip To: End of Survey If I am am a PhD candidate at the University of Plymouth in the School of Computing. I am conducting... != I consent, begin the study

End of Block: First page

Start of Block: Section 1: Demographic Information

Section 1: Demographic Information

What is your gender?

- ○ Male
- ○ Female

What is your age?

- ○ 18 - 24
- ○ 25 - 34
- ○ 35 - 44
- ○ 45 - 54
- ○ 55 - 64
- ○ 65 or older

What is the highest level of school you have completed or the highest degree you have received?

- ○ Less than high school qualifications
- ○ High school qualifications (e.g GSCE)
- ○ College certificate (e.g A- Levels, GNVQ)
- ○ Bachelor degree
- ○ Postgraduate degree

Page Break

End of Block: Section 1: Demographic Information

Start of Block: Section 2: Cyber Security Experience and Knowledge

Section 2: Cyber Security Experience and Knowledge

How would you rate your technology experience?

- ○ Novice
- ○ Advanced Beginner
- ○ Competent
- ○ Proficient
- ○ Expert

Read each statement carefully and indicate your level of concern with the following statements about the security of your digital devices: (all the below statements are related to your digital devices)

	Extremely concerned	Very concerned	Moderately concerned	Slightly concerned	Not concerned at all
A. Security and safety for all your digital devices	○	○	○	○	○
B. Security and safety for all the digital devices owned and used by your family	○	○	○	○	○
C. Password security settings and configuration.	○	○	○	○	○
D. Antivirus software settings and update.	○	○	○	○	○
E. The operating system security settings and updates	○	○	○	○	○
F. The Internet browser security settings.	○	○	○	○	○
G. The backup configuration settings.	○	○	○	○	○
H. The applications security and management in your digital devices.	○	○	○	○	○
I. The security configuration settings of the internet modem.	○	○	○	○	○
J. Parental controls and purchasing security settings.	○	○	○	○	○

Read each statement carefully and indicate your level of knowledge with the following statements about the security of your digital devices: (all the below statements are related to your digital devices)

	Extremely knowledgeable	Very knowledgeable	Moderately knowledgeable	Slightly knowledgeable	Not knowledgeable at all
A. Security and safety for all your digital devices	○	○	○	○	○
B. Security and safety for all the digital devices owned and used by your family	○	○	○	○	○
C. Password security settings and configuration.	○	○	○	○	○
D. Antivirus software settings and update.	○	○	○	○	○
E. The operating system security settings and updates	○	○	○	○	○
F. The Internet browser security settings.	○	○	○	○	○
G. The backup configuration settings.	○	○	○	○	○
H. The applications security and management in your digital devices.	○	○	○	○	○
I. The security configuration settings of the internet modem.	○	○	○	○	○
J. Parental controls and purchasing security settings.	○	○	○	○	○

Read each statement carefully and indicate how often do you manage / control / configure the the following security settings of your digital devices: (all the below statements are related to your digital devices)

	Always	Very often	Sometimes	Rarely	Never
A. Security and safety for all your digital devices.	○	○	○	○	○
B. Security and safety for all the digital devices owned and used by your family.	○	○	○	○	○
C. Password security settings and configuration.	○	○	○	○	○
D. Antivirus software settings and update.	○	○	○	○	○
E. The operating system security settings and updates	○	○	○	○	○
F. The Internet browser security settings.	○	○	○	○	○
G. The backup configuration settings.	○	○	○	○	○
H. The applications security and management in your digital devices.	○	○	○	○	○
I. The security configuration settings of the internet modem.	○	○	○	○	○
J. Parental controls and purchasing security settings.	○	○	○	○	○

Read each statement carefully and indicate how easy or difficult is to manage / control / configure the the following:

	Extremely easy	Somewhat easy	Neither easy nor difficult	Somewhat difficult	Extremely difficult
A. Security and safety for all your digital devices	○	○	○	○	○
B. Security and safety for all the digital devices owned and used by your family	○	○	○	○	○
C. Password security settings and configuration.	○	○	○	○	○
D. Antivirus software settings and update.	○	○	○	○	○
E. The operating system security settings and updates	○	○	○	○	○
F. The Internet browser security settings.	○	○	○	○	○
G. The backup configuration settings.	○	○	○	○	○
H. The applications security and management in your digital devices.	○	○	○	○	○
I. The security configuration settings of the internet modem.	○	○	○	○	○
J. Parental controls and purchasing security settings	○	○	○	○	○

Read each statement carefully and indicate your level of agreement with the following statements about the security of the digital devices:

	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
Different level of security settings should be applied to all the digital devices. (such as low, medium and high level)	○	○	○	○	○
Different security settings should be implemented and focused upon the user rather than the device	○	○	○	○	○
One security level should be applied on all the devices belongs to one user?	○	○	○	○	○
It would be a good idea to have pre-defined templates of security setting	○	○	○	○	○

Page Break

End of Block: Section 2 : Cyber Security Experience and Knowledge

Start of Block: Section 3: Information Security Management System

Section 3: Information Security Management System:

The previous studies and researches indicate that there is a lack in providing the home users with a customised awareness content based on their current needs and the threats that may they experience. This approach can be done by applying different groups of information security policies based on the technologies, applications, and services which are used.

A number of policies will be proposed to manage and monitor the security configuration and practice in different technologies and digital devices:

1. Password policy: it contains the most common password configurations which are applicable to be implemented in the devices such as password complexity and minimum password length.

2. Device Security policy: it includes the most important features in the devices which need to be managed effectively in order to harden the security of the devices. For example, virus protection and up-to-date OS version.

3. Software security policy: it is responsible for managing and controlling all the configuration and settings related to the installation of the applications and software such as applications auto update and installing apps from unknown sources.

4. Internet browser policy: it has all the main security settings which need to be monitored and restricted in all the most popular internet browsers such as Pop-Ups blocker and saving login information.

5. Backup policy: it covers all the configurations which can help the users to restore the original data after a data loss event such as backup schedule and setup.

The proposed system will have usable user interfaces which can help in managing the devices effectively, increasing the security awareness and reducing the potential threats. The proposed architecture which will begin by identifying the users and technologies used within the home network. Next, appropriate policies can be assigned to the digital devices. Once the device get enrolled, the security settings and controls configured in the device will be checked in order to be compared with assigned policies. The users will be notified with appropriate awareness content if there is a vulnerability which could lead to a possible threat.

The proposed system consists of several main sections such as dashboard section,

enrolment section, management section and agents.

You are going now to evaluate different interfaces in terms of the functionality and the usability aspects:

End of Block: Section 3: Information Security Management System

Start of Block: Section 3.1: The main dashboard interface of the management system

Section 3.1: The main dashboard interface of the management system:

The main aim of the dashboard is to notify the administrator in a good method about:

- The current users.
- The devices compliance.
- The security alerts.
- The latest changes or updates.

Now , you are going to review two initial interfaces which are designed for the main dashboard

The first interface:

The interface contains several sections which can provide the administrator with different notifications and alerts:

- Security Settings Alert: shows the current status of several scurity settings in the managed ddevices.
- Activity Feed: shows a list of recent activities performed in the system and the managed devices.
- Users and devices: shows the security status of the managed devices for each user.
- Security Compliance: shows the compliance of several security policies for the devices.

Please, read each statement carefully and rate each point based on the above interface:

	Excellent	Very good	Good	Fair	Poor
A. The structure of the interface	○	○	○	○	○
B. The colours used in the dashboard	○	○	○	○	○
C. The text font and size	○	○	○	○	○
D. The icons used in the dashboard	○	○	○	○	○
E. The visuality of the dashboard	○	○	○	○	○
F. The coherence of the appearance	○	○	○	○	○
G. The sequence of the sections	○	○	○	○	○
H. The understanding of each section	○	○	○	○	○
I. The ease of use	○	○	○	○	○
J. The relevance of the information	○	○	○	○	○

Comment:

_____

_____

_____

_____

_____

The second interface:

The interface contains several sections which can provide the administrator with different notifications and alerts:

- Security Settings Alert: shows the current status of several security settings in the managed devices.
- Activity Feed: shows a list of recent activities performed in the system and the managed devices.
- Users and devices: shows the security status of the managed devices for each user.
- Security Compliance by users : shows the compliance status of all the digital devices owned by each user.
- Security Compliance by devices: shows the compliance status for each individual device.

Please, read each statement carefully and rate each point based on the above interface:

	Excellent	Very good	Good	Fair	Poor
A. The structure of the interface	○	○	○	○	○
B. The colours used in the dashboard	○	○	○	○	○
C. The text font and size	○	○	○	○	○
D. The icons used in the dashboard	○	○	○	○	○
E. The visuality of the dashboard	○	○	○	○	○
F. The coherence of the appearance	○	○	○	○	○
G. The sequence of the sections	○	○	○	○	○
H. The understanding of each section	○	○	○	○	○
I. The ease of use	○	○	○	○	○
J. The relevance of the information	○	○	○	○	○

Comment:

_____

_____

_____

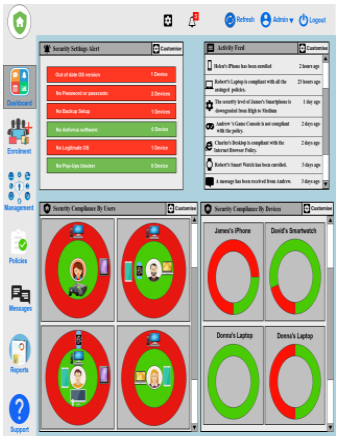
_____

_____

Which interface would you prefer?

○ The first interface

○ The second interface



End of Block: Section 3.1 : The main dashboard interface of the management system

Start of Block: Section 3.2: The enrolment interface

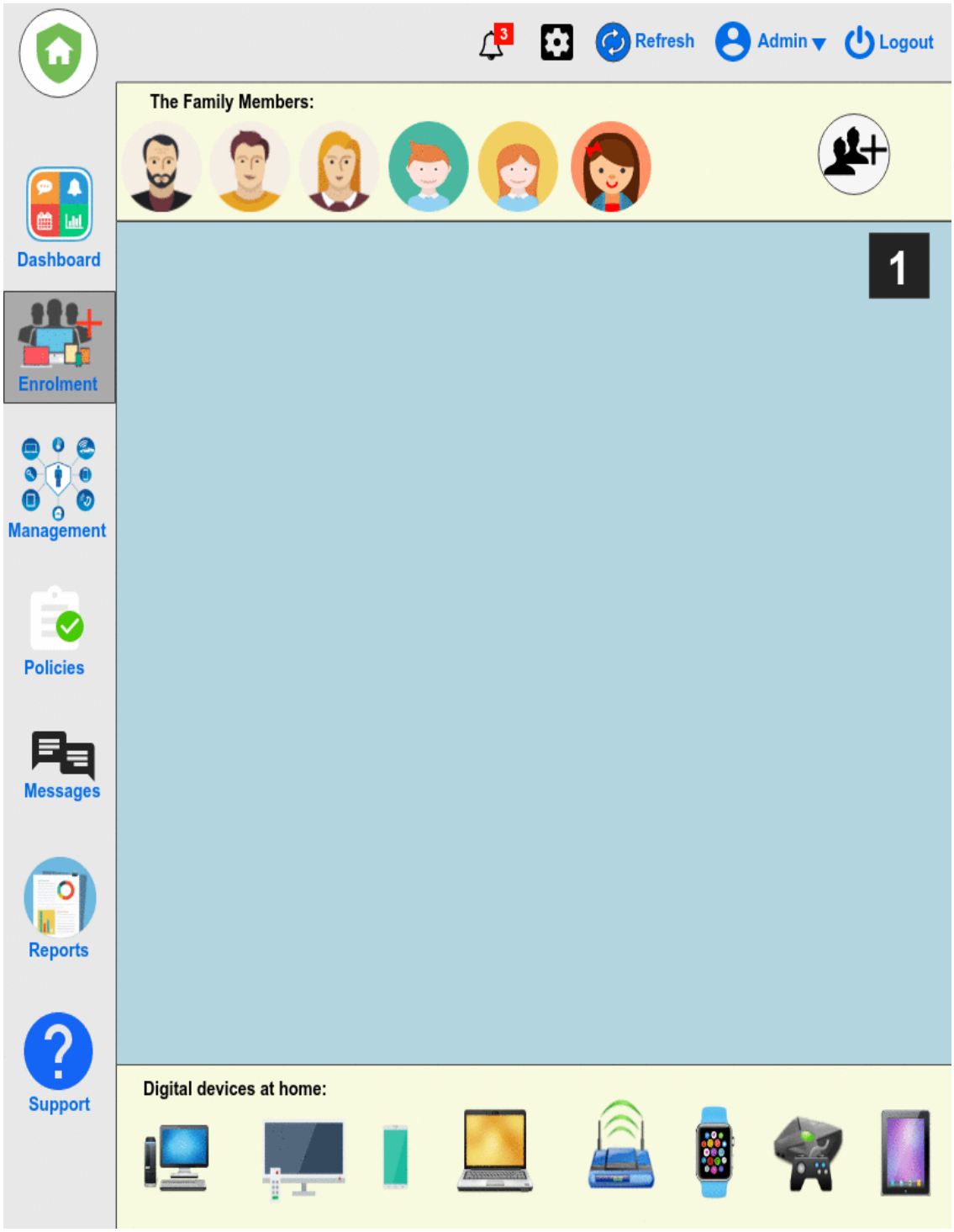
Section 3.2: The enrolment interface:

The administrator can start the process of the enrolment for adding new users and devices by creating new profiles including:

- Users.
- Devices.
- Security Policies.
- Security Level

The first Interface (Drag-and-Drop approach):

This interface is designed by using the feature of Drag-and -Drop technique. the first step in the enrolment is that the administrator should select a user and a device by grabbing and dropping them blue area. Next, a popup window will be appeared which asks for selecting a platform, security policies and the security level.



Please, read each statement carefully and rate each point based on the above interface:

	Excellent	Very good	Good	Fair	Poor
A. The structure of the interface	○	○	○	○	○
B. The colours used in the dashboard	○	○	○	○	○
C. The text font and size	○	○	○	○	○
D. The icons used in the dashboard	○	○	○	○	○
E. The visuality of the dashboard	○	○	○	○	○
F. The coherence of the appearance	○	○	○	○	○
G. The sequence of the sections	○	○	○	○	○
H. The understanding of each section	○	○	○	○	○
I. The ease of use	○	○	○	○	○
J. The relevance of the information	○	○	○	○	○

Comment:

_____

_____

_____

_____

The second interface (Point-and-Click approach):

It is designed by utilising the approach of Point-and-Click. Firstly, the user should move the pointer and click cover a specific user and device. Next, the required security polices and level can be selected. Finally the invitation will be sent to the user in order to finalise the enrolment process.

Please, read each statement carefully and rate each point based on the above interface:

	Excellent	Very good	Good	Fair	Poor
A. The structure of the interface	○	○	○	○	○
B. The colours used in the dashboard	○	○	○	○	○
C. The text font and size	○	○	○	○	○
D. The icons used in the dashboard	○	○	○	○	○
E. The visuality of the dashboard	○	○	○	○	○
F. The coherence of the appearance	○	○	○	○	○
G. The sequence of the sections	○	○	○	○	○
H. The understanding of each section	○	○	○	○	○
I. The ease of use	○	○	○	○	○
J. The relevance of the information	○	○	○	○	○

Comment:

_____

_____

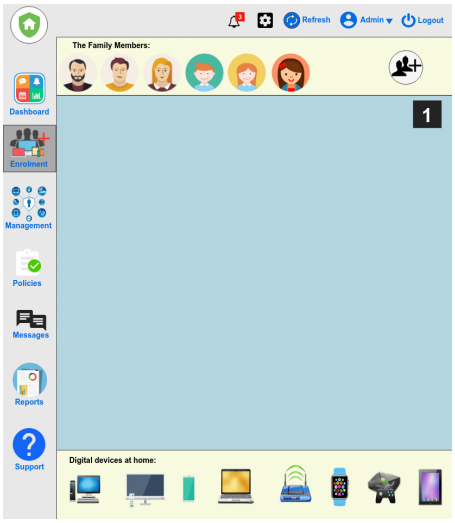
_____

_____

_____

Which interface would you prefer?

○ Interface 1 (Drag-and-Drop approach)



○ Interface 2 (Point-and-Click approach)

Page Break

End of Block: Section 3.2: The enrolment interface

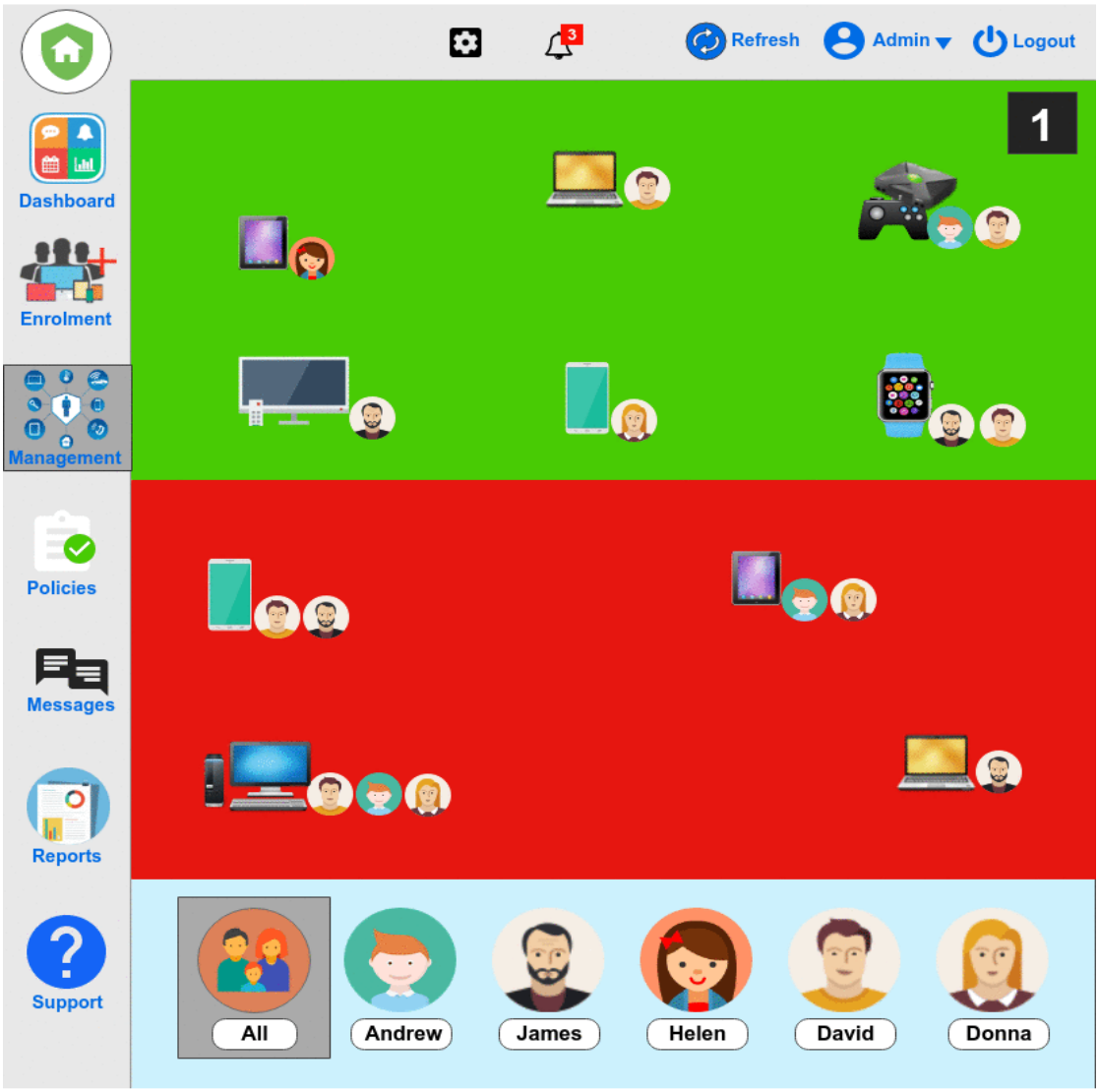
Start of Block: Section 3.3: The management interface:

Section 3.3: The management interface:

The management section is responsible for managing, monitoring and checking the compliance of the enrolled devices with their assigned policies. Several tasks can be done via the management interface such as viewing profiles, changing the assigned policies, changing the owner and sending messages to the users.

The First interface (Red and Green):

The interface is designed by providing two areas: the red area represents the non-compliant devices and the green area for the compliant devices.



Please, read each statement carefully and rate each point based on the above interface:

	Excellent	Very good	Good	Fair	Poor
A. The structure of the interface	○	○	○	○	○
B. The colours used in the dashboard	○	○	○	○	○
C. The text font and size	○	○	○	○	○
D. The icons used in the dashboard	○	○	○	○	○
E. The visuality of the dashboard	○	○	○	○	○
F. The coherence of the appearance	○	○	○	○	○
G. The sequence of the sections	○	○	○	○	○
H. The understanding of each section	○	○	○	○	○
I. The ease of use	○	○	○	○	○
J. The relevance of the information	○	○	○	○	○

Comment:

_____

_____

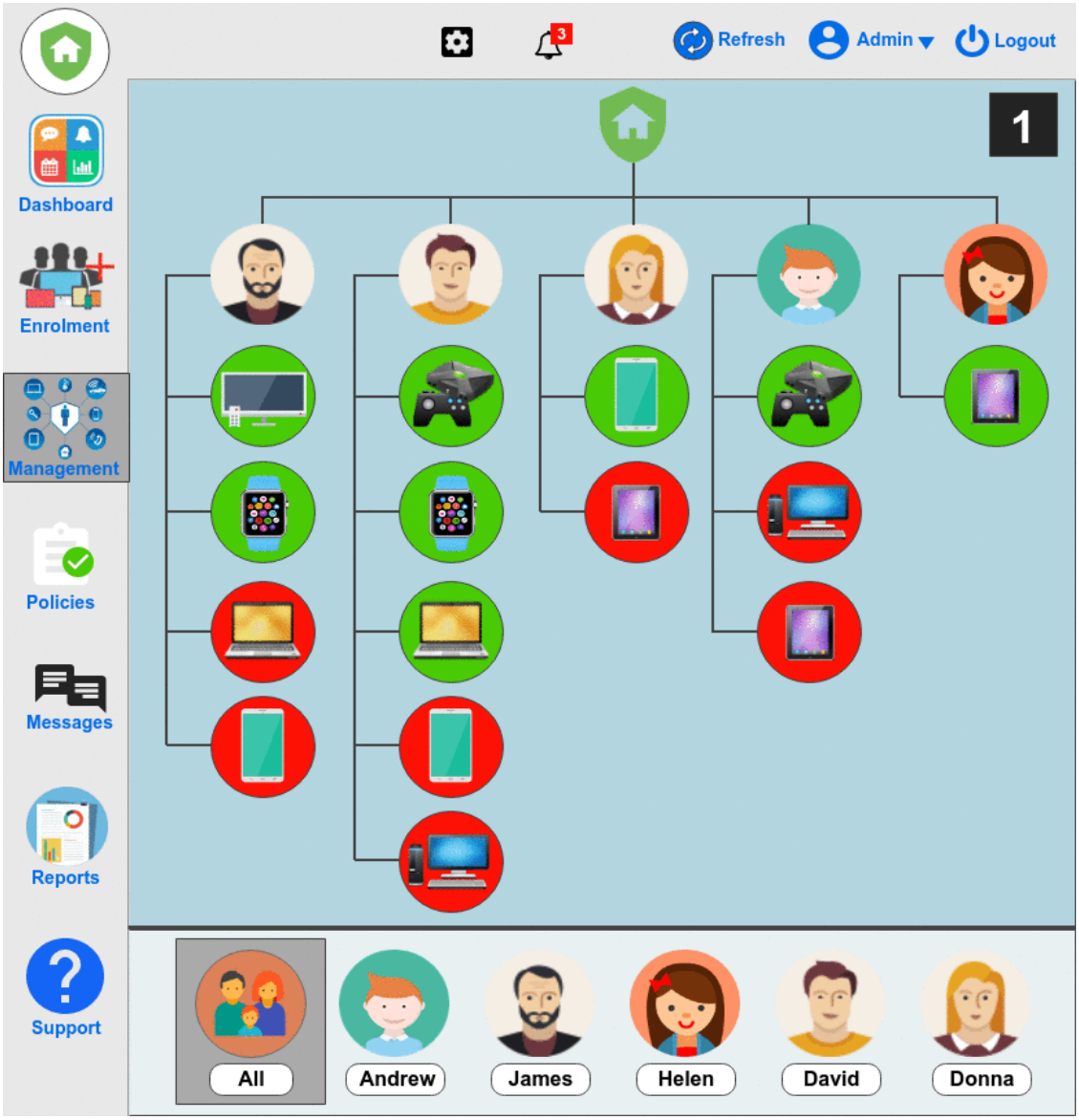
_____

_____

_____

The second interface (hierarchical style):

The interface is designed based on a hierarchical style which can give a comprehensive overview and management for all the enrolled devices: the non-compliant devices will have a red circle and the compliant devices will have green.



Please, read each statement carefully and rate each point based on the above interface:

	Excellent	Very good	Good	Fair	Poor
A. The structure of the interface	○	○	○	○	○
B. The colours used in the dashboard	○	○	○	○	○
C. The text font and size	○	○	○	○	○
D. The icons used in the dashboard	○	○	○	○	○
E. The visuality of the dashboard	○	○	○	○	○
F. The coherence of the appearance	○	○	○	○	○
G. The sequence of the sections	○	○	○	○	○
H. The understanding of each section	○	○	○	○	○
I. The ease of use	○	○	○	○	○
J. The relevance of the information	○	○	○	○	○

Comment:

_____

_____

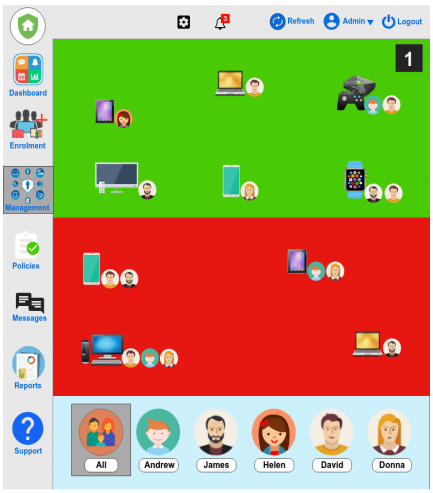
_____

_____

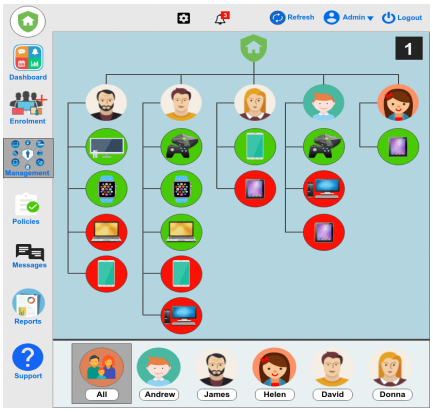
_____

Which interface would you prefer?

○ Interface 1 (Red and Green)



○ Interface 2 (hierarchical style)



User Profile:

Once the administrator click on the option of viewing profile in one of the previous interfaces, a comprehensive detail about the status of the device compliance will be provided in a usable way including:

- Latest alerts
- Send messages
- Change security level
- Change device owner
- Recent activities performed on the device
- Profile summary which can show the security status of the device.
- Information about the assigned security policies

The first interface (horizontal menu):

The interface is designed to present the security policies in a horizontal menu with red and green icons to assist the administrator.

Please, read each statement carefully and rate each point based on the above interface:

	Excellent	Very good	Good	Fair	Poor
A. The structure of the interface	○	○	○	○	○
B. The colours used in the dashboard	○	○	○	○	○
C. The text font and size	○	○	○	○	○
D. The icons used in the dashboard	○	○	○	○	○
E. The visuality of the dashboard	○	○	○	○	○
F. The coherence of the appearance	○	○	○	○	○
G. The sequence of the sections	○	○	○	○	○
H. The understanding of each section	○	○	○	○	○
I. The ease of use	○	○	○	○	○
J. The relevance of the information	○	○	○	○	○

Comment:

_____

_____

_____

_____

_____

The second interface (clickable boxes):

It is designed to present the security policies in clickable boxes and each box will be coloured with green or red to show the user compliance.

Please, read each statement carefully and rate each point based on the above interface:

	Excellent	Very good	Good	Fair	Poor
A. The structure of the interface	○	○	○	○	○
B. The colours used in the dashboard	○	○	○	○	○
C. The text font and size	○	○	○	○	○
D. The icons used in the dashboard	○	○	○	○	○
E. The visuality of the dashboard	○	○	○	○	○
F. The coherence of the appearance	○	○	○	○	○
G. The sequence of the sections	○	○	○	○	○
H. The understanding of each section	○	○	○	○	○
I. The ease of use	○	○	○	○	○
J. The relevance of the information	○	○	○	○	○

Comment:

_____

_____

_____

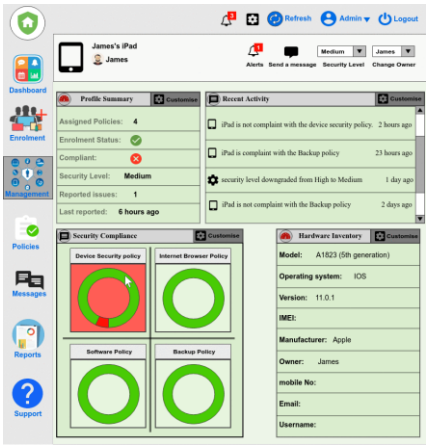
_____

_____

Which interface would you prefer?

○ Interface 1 (horizontal menu)

○ Interface 2 (clickable boxes)



Page Break

End of Block: Section 3.3: The management interface:

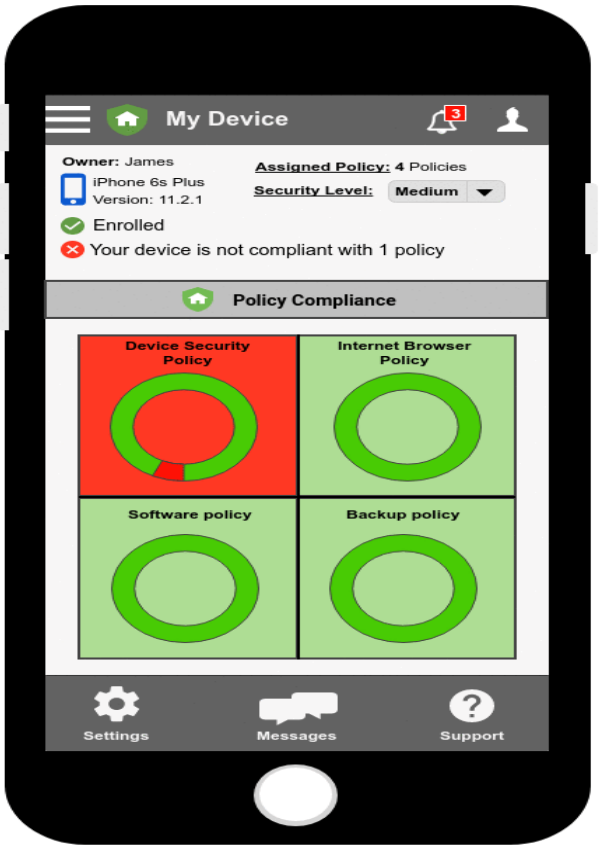
Start of Block: Section 3.4: The agent interfaces

Section 3.4: The Agent Interface:

The main duty of the agent is to provide a communication between the devices and the management security system, including:

- Scan
- check
- capture
- send notifications and a summary about the status of the device.

The first interface (clickable boxes):
It is designed to show the assigned security policies in clickable boxes with red or green colour to reflect the user compliance with each policy.



Please, read each statement carefully and rate each point based on the above interface:

	Excellent	Very good	Good	Fair	Poor
A. The structure of the interface	○	○	○	○	○
B. The colours used in the dashboard	○	○	○	○	○
C. The text font and size	○	○	○	○	○
D. The icons used in the dashboard	○	○	○	○	○
E. The visuality of the dashboard	○	○	○	○	○
F. The coherence of the appearance	○	○	○	○	○
G. The sequence of the sections	○	○	○	○	○
H. The understanding of each section	○	○	○	○	○
I. The ease of use	○	○	○	○	○
J. The relevance of the information	○	○	○	○	○

Comment:

_____

_____

_____

_____

_____

The second interface (Expandable/Collapsible Sections):
It is designed to present the assigned security policies in expandable/collapsible sections which can make it easy for the user to move between the sections.

Please, read each statement carefully and rate each point based on the above interface:

	Excellent	Very good	Good	Fair	Poor
A. The structure of the interface	○	○	○	○	○
B. The colours used in the dashboard	○	○	○	○	○
C. The text font and size	○	○	○	○	○
D. The icons used in the dashboard	○	○	○	○	○
E. The visuality of the dashboard	○	○	○	○	○
F. The coherence of the appearance	○	○	○	○	○
G. The sequence of the sections	○	○	○	○	○
H. The understanding of each section	○	○	○	○	○
I. The ease of use	○	○	○	○	○
J. The relevance of the information	○	○	○	○	○

Q Comment:

_____

_____

_____

_____

_____

Which interface would you prefer?

○ Interface 1 (Clickable boxes)

○ Interface 2 (Expandable/Collapsible Sections)

End of Block: Section 3.4: The agent interfaces

Appendix B: Ethical Approval (User Survey)

UNIVERSITY OF PLYMOUTH

8 August 2018

CONFIDENTIAL
Fayez Alotaibi
School of Computing, Electronics and Mathematics

Dear Fayez

Ethical Approval Application

Thank you for submitting the ethical approval form and details concerning your project:

Information Security Management for Home Users

I am pleased to inform you that this has been approved.

Kind regards

Paula Simson
Secretary to Faculty Research Ethics Committee

Cc. Prof Nathan Clarke
Prof Steven Furnell

Mrs Jayne Brenen, Head of Faculty Operations, Faculty of Science and Engineering, University of Plymouth, Drake Circus, Plymouth, Devon PL4 8AA T +44 (0)1752 584584 F +44 (0)1752 584540 W www.plymouth.ac.uk

Appendix C: Ethical approval (Focus Groups)

UNIVERSITY OF PLYMOUTH

3rd July 2019

CONFIDENTIAL
Fayez Alotaibi
School of Computing, Electronics and Mathematics

Dear Fayez

Ethical Approval Application

Thank you for submitting the ethical approval form and details concerning your project:

Information Security management for Home Users

I am pleased to inform you that this has been approved.
Kind regards

Steven Neal
Secretary to Faculty Research Ethics Committee

Mrs Jayne Brenen, Head of Faculty Operations, Faculty of Science and Engineering, University of Plymouth, Drake Circus, Plymouth, Devon PL4 8AA T +44 (0)1752 584584 F +44 (0)1752 584540 W www.plymouth.ac.uk

Appendix D: SPSS Results

		age
age	Pearson Correlation	1
	Sig. (2-tailed)	
	N	434
Concern: Security and safety for all the digital devices used by you	Pearson Correlation	.093
	Sig. (2-tailed)	.052
	N	434
Concern: Security and safety for all the digital devices used by your family members	Pearson Correlation	.029
	Sig. (2-tailed)	.546
	N	434
Concern: Password security settings.	Pearson Correlation	.068
	Sig. (2-tailed)	.160
	N	434
Concern: Antivirus software settings.	Pearson Correlation	.088
	Sig. (2-tailed)	.066
	N	434
Concern: The operating system security settings	Pearson Correlation	.135**
	Sig. (2-tailed)	.005
	N	434
Concern: The Internet browser security settings.	Pearson Correlation	.036
	Sig. (2-tailed)	.457
	N	434
Concern: The backup configuration settings.	Pearson Correlation	.064
	Sig. (2-tailed)	.182
	N	434
Concern: The applications security and management in your digital devices.	Pearson Correlation	.097*
	Sig. (2-tailed)	.044
	N	434
Concern: The security configuration settings of the access points (modem)	Pearson Correlation	.099*
	Sig. (2-tailed)	.039
	N	434
Concern: Parental control settings.	Pearson Correlation	.230**
	Sig. (2-tailed)	.000
	N	434

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

		age
age	Pearson Correlation	1
	Sig. (2-tailed)	
	N	434
Knowledge: Security and safety for all the digital devices used by you	Pearson Correlation	-.011
	Sig. (2-tailed)	.827
	N	434
Knowledge: Security and safety for all the digital devices used by your family members	Pearson Correlation	.139**
	Sig. (2-tailed)	.004
	N	434
Knowledge: Password security settings.	Pearson Correlation	-.035
	Sig. (2-tailed)	.465
	N	434
Knowledge: Antivirus software settings.	Pearson Correlation	.081
	Sig. (2-tailed)	.093
	N	434
Knowledge: The operating system security settings.	Pearson Correlation	.017
	Sig. (2-tailed)	.717
	N	434
Knowledge: The Internet browser security settings.	Pearson Correlation	.001
	Sig. (2-tailed)	.980
	N	434
Knowledge: The backup configuration settings.	Pearson Correlation	-.025
	Sig. (2-tailed)	.600
	N	434
Knowledge: The applications security and management in your digital devices.	Pearson Correlation	.056
	Sig. (2-tailed)	.247
	N	434
Knowledge: The security configuration settings of the access points (modem).	Pearson Correlation	.122*
	Sig. (2-tailed)	.011
	N	434
Knowledge: Parental controls settings.	Pearson Correlation	.084
	Sig. (2-tailed)	.079
	N	434

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

		age
age	Pearson Correlation	1
	Sig. (2-tailed)	
	N	434
management: Security and safety for all the digital devices used by you	Pearson Correlation	.012
	Sig. (2-tailed)	.802
	N	434
management: Security and safety for all the digital devices used by your family members	Pearson Correlation	.168**
	Sig. (2-tailed)	.000
	N	434
management: Password security settings.	Pearson Correlation	-.064
	Sig. (2-tailed)	.181
	N	434
management: Antivirus software settings.	Pearson Correlation	.070
	Sig. (2-tailed)	.144
	N	434
management: The operating system security settings.	Pearson Correlation	.047
	Sig. (2-tailed)	.328
	N	434
management: The Internet browser security settings.	Pearson Correlation	.006
	Sig. (2-tailed)	.906
	N	434
management: The backup configuration settings.	Pearson Correlation	.010
	Sig. (2-tailed)	.828
	N	434
management: The applications security and management in your digital devices.	Pearson Correlation	-.049
	Sig. (2-tailed)	.312
	N	434
management: The security configuration settings of the access points (modem).	Pearson Correlation	.069
	Sig. (2-tailed)	.150
	N	434
management: Parental control settings.	Pearson Correlation	.165**
	Sig. (2-tailed)	.001
	N	434

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

		age
age	Pearson Correlation	1

	Sig. (2-tailed)	
	N	434
Ease: Security and safety for all the digital devices used by you.	Pearson Correlation	-.130**
	Sig. (2-tailed)	.008
	N	422
Ease: Security and safety for all the digital devices used by your family members.	Pearson Correlation	.083
	Sig. (2-tailed)	.099
	N	394
Ease: Password security settings.	Pearson Correlation	-.111*
	Sig. (2-tailed)	.023
	N	420
Ease: Antivirus software settings.	Pearson Correlation	-.022
	Sig. (2-tailed)	.656
	N	400
Ease: The operating system security settings.	Pearson Correlation	-.060
	Sig. (2-tailed)	.229
	N	397
Ease: The Internet browser security settings.	Pearson Correlation	-.101*
	Sig. (2-tailed)	.045
	N	394
Ease:The backup configuration settings.	Pearson Correlation	-.158**
	Sig. (2-tailed)	.002
	N	387
Ease: The applications security and management in your digital devices.	Pearson Correlation	-.099*
	Sig. (2-tailed)	.048
	N	397
Ease: The security configuration settings of the access points (modem).	Pearson Correlation	-.078
	Sig. (2-tailed)	.133
	N	370
Ease: Parental control settings.	Pearson Correlation	-.039
	Sig. (2-tailed)	.463
	N	363

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

		Education
Education	Pearson Correlation	1

	Sig. (2-tailed)	
	N	434
Concern: Security and safety for all the digital devices used by you	Pearson Correlation	.098*
	Sig. (2-tailed)	.042
	N	434
Concern: Security and safety for all the digital devices used by your family members	Pearson Correlation	.042
	Sig. (2-tailed)	.388
	N	434
Concern: Password security settings.	Pearson Correlation	.070
	Sig. (2-tailed)	.146
	N	434
Concern: Antivirus software settings.	Pearson Correlation	.048
	Sig. (2-tailed)	.316
	N	434
Concern: The operating system security settings	Pearson Correlation	.066
	Sig. (2-tailed)	.171
	N	434
Concern: The Internet browser security settings.	Pearson Correlation	.043
	Sig. (2-tailed)	.376
	N	434
Concern: The backup configuration settings.	Pearson Correlation	.055
	Sig. (2-tailed)	.250
	N	434
Concern: The applications security and management in your digital devices.	Pearson Correlation	.038
	Sig. (2-tailed)	.428
	N	434
Concern: The security configuration settings of the access points (modem)	Pearson Correlation	.050
	Sig. (2-tailed)	.300
	N	434
Concern: Parental control settings.	Pearson Correlation	.070
	Sig. (2-tailed)	.144
	N	434

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

		Education
Education	Pearson Correlation	1
	Sig. (2-tailed)	

	N	434
Knowledge: Security and safety for all the digital devices used by you	Pearson Correlation	-.040
	Sig. (2-tailed)	.412
	N	434
Knowledge: Security and safety for all the digital devices used by your family members	Pearson Correlation	.124**
	Sig. (2-tailed)	.010
	N	434
Knowledge: Password security settings.	Pearson Correlation	.009
	Sig. (2-tailed)	.859
	N	434
Knowledge: Antivirus software settings.	Pearson Correlation	.120*
	Sig. (2-tailed)	.012
	N	434
Knowledge: The operating system security settings.	Pearson Correlation	-.003
	Sig. (2-tailed)	.944
	N	434
Knowledge: The Internet browser security settings.	Pearson Correlation	.014
	Sig. (2-tailed)	.777
	N	434
Knowledge: The backup configuration settings.	Pearson Correlation	-.016
	Sig. (2-tailed)	.746
	N	434
Knowledge: The applications security and management in your digital devices.	Pearson Correlation	-.031
	Sig. (2-tailed)	.515
	N	434
Knowledge: The security configuration settings of the access points (modem).	Pearson Correlation	.056
	Sig. (2-tailed)	.243
	N	434
Knowledge: Parental controls settings.	Pearson Correlation	.085
	Sig. (2-tailed)	.078
	N	434

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

		Education
management: Security and safety for all the digital devices used by you	Pearson Correlation	-.007
	Sig. (2-tailed)	.881
	N	434

management: Security and safety for all the digital devices used by your family members	Pearson Correlation	.062
	Sig. (2-tailed)	.194
	N	434
management: Password security settings.	Pearson Correlation	-.040
	Sig. (2-tailed)	.402
	N	434
management: Antivirus software settings.	Pearson Correlation	.045
	Sig. (2-tailed)	.350
	N	434
management: The operating system security settings.	Pearson Correlation	-.010
	Sig. (2-tailed)	.830
	N	434
management: The Internet browser security settings.	Pearson Correlation	.005
	Sig. (2-tailed)	.923
	N	434
management: The backup configuration settings.	Pearson Correlation	.028
	Sig. (2-tailed)	.559
	N	434
management: The applications security and management in your digital devices.	Pearson Correlation	-.097*
	Sig. (2-tailed)	.043
	N	434
management: The security configuration settings of the access points (modem).	Pearson Correlation	-.009
	Sig. (2-tailed)	.847
	N	434
management: Parental control settings.	Pearson Correlation	.067
	Sig. (2-tailed)	.164
	N	434

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

		Education
Ease: Security and safety for all the digital devices used by you.	Pearson Correlation	-.070
	Sig. (2-tailed)	.151
	N	422

Ease: Security and safety for all the digital devices used by your family members.	Pearson Correlation	-.046
	Sig. (2-tailed)	.358
	N	394
Ease: Password security settings.	Pearson Correlation	-.070
	Sig. (2-tailed)	.153
	N	420
Ease: Antivirus software settings.	Pearson Correlation	.023
	Sig. (2-tailed)	.651
	N	400
Ease: The operating system security settings.	Pearson Correlation	-.066
	Sig. (2-tailed)	.191
	N	397
Ease: The Internet browser security settings.	Pearson Correlation	-.064
	Sig. (2-tailed)	.202
	N	394
Ease:The backup configuration settings.	Pearson Correlation	-.116*
	Sig. (2-tailed)	.023
	N	387
Ease: The applications security and management in your digital devices.	Pearson Correlation	-.073
	Sig. (2-tailed)	.149
	N	397
Ease: The security configuration settings of the access points (modem).	Pearson Correlation	-.149**
	Sig. (2-tailed)	.004
	N	370
Ease: Parental control settings.	Pearson Correlation	-.089
	Sig. (2-tailed)	.089
	N	363

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

		IT experience
IT experience	Pearson Correlation	1
	Sig. (2-tailed)	
	N	434

Concern: Security and safety for all the digital devices used by you	Pearson Correlation	.210**
	Sig. (2-tailed)	.000
	N	434
Concern: Security and safety for all the digital devices used by your family members	Pearson Correlation	.114*
	Sig. (2-tailed)	.017
	N	434
Concern: Password security settings.	Pearson Correlation	.115*
	Sig. (2-tailed)	.016
	N	434
Concern: Antivirus software settings.	Pearson Correlation	.052
	Sig. (2-tailed)	.281
	N	434
Concern: The operating system security settings	Pearson Correlation	.134**
	Sig. (2-tailed)	.005
	N	434
Concern: The Internet browser security settings.	Pearson Correlation	.087
	Sig. (2-tailed)	.070
	N	434
Concern: The backup configuration settings.	Pearson Correlation	.021
	Sig. (2-tailed)	.669
	N	434
Concern: The applications security and management in your digital devices.	Pearson Correlation	.102*
	Sig. (2-tailed)	.033
	N	434
Concern: The security configuration settings of the access points (modem)	Pearson Correlation	.131**
	Sig. (2-tailed)	.006
	N	434
Concern: Parental control settings.	Pearson Correlation	.097*
	Sig. (2-tailed)	.043
	N	434

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

		IT experience
IT experience	Pearson Correlation	1
	Sig. (2-tailed)	
	N	434

Knowledge: Security and safety for all the digital devices used by you	Pearson Correlation	.432**
	Sig. (2-tailed)	.000
	N	434
Knowledge: Security and safety for all the digital devices used by your family members	Pearson Correlation	.367**
	Sig. (2-tailed)	.000
	N	434
Knowledge: Password security settings.	Pearson Correlation	.245**
	Sig. (2-tailed)	.000
	N	434
Knowledge: Antivirus software settings.	Pearson Correlation	.351**
	Sig. (2-tailed)	.000
	N	434
Knowledge: The operating system security settings.	Pearson Correlation	.345**
	Sig. (2-tailed)	.000
	N	434
Knowledge: The Internet browser security settings.	Pearson Correlation	.368**
	Sig. (2-tailed)	.000
	N	434
Knowledge: The backup configuration settings.	Pearson Correlation	.343**
	Sig. (2-tailed)	.000
	N	434
Knowledge: The applications security and management in your digital devices.	Pearson Correlation	.358**
	Sig. (2-tailed)	.000
	N	434
Knowledge: The security configuration settings of the access points (modem).	Pearson Correlation	.372**
	Sig. (2-tailed)	.000
	N	434
Knowledge: Parental controls settings.	Pearson Correlation	.286**
	Sig. (2-tailed)	.000
	N	434

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

		IT experience
IT experience	Pearson Correlation	1
	Sig. (2-tailed)	
	N	434

management: Security and safety for all the digital devices used by you	Pearson Correlation	.248**
	Sig. (2-tailed)	.000
	N	434
management: Security and safety for all the digital devices used by your family members	Pearson Correlation	.251**
	Sig. (2-tailed)	.000
	N	434
management: Password security settings.	Pearson Correlation	.191**
	Sig. (2-tailed)	.000
	N	434
management: Antivirus software settings.	Pearson Correlation	.243**
	Sig. (2-tailed)	.000
	N	434
management: The operating system security settings.	Pearson Correlation	.244**
	Sig. (2-tailed)	.000
	N	434
management: The Internet browser security settings.	Pearson Correlation	.245**
	Sig. (2-tailed)	.000
	N	434
management: The backup configuration settings.	Pearson Correlation	.217**
	Sig. (2-tailed)	.000
	N	434
management: The applications security and management in your digital devices.	Pearson Correlation	.235**
	Sig. (2-tailed)	.000
	N	434
management: The security configuration settings of the access points (modem).	Pearson Correlation	.227**
	Sig. (2-tailed)	.000
	N	434
management: Parental control settings.	Pearson Correlation	.237**
	Sig. (2-tailed)	.000
	N	434

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

		IT experience
IT experience	Pearson Correlation	1
	Sig. (2-tailed)	
	N	434

Ease: Security and safety for all the digital devices used by you.	Pearson Correlation	.182**
	Sig. (2-tailed)	.000
	N	422
Ease: Security and safety for all the digital devices used by your family members.	Pearson Correlation	.171**
	Sig. (2-tailed)	.001
	N	394
Ease: Password security settings.	Pearson Correlation	.021
	Sig. (2-tailed)	.674
	N	420
Ease: Antivirus software settings.	Pearson Correlation	.150**
	Sig. (2-tailed)	.003
	N	400
Ease: The operating system security settings.	Pearson Correlation	.154**
	Sig. (2-tailed)	.002
	N	397
Ease: The Internet browser security settings.	Pearson Correlation	.251**
	Sig. (2-tailed)	.000
	N	394
Ease:The backup configuration settings.	Pearson Correlation	.144**
	Sig. (2-tailed)	.004
	N	387
Ease: The applications security and management in your digital devices.	Pearson Correlation	.144**
	Sig. (2-tailed)	.004
	N	397
Ease: The security configuration settings of the access points (modem).	Pearson Correlation	.111*
	Sig. (2-tailed)	.033
	N	370
Ease: Parental control settings.	Pearson Correlation	.075
	Sig. (2-tailed)	.156
	N	363

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

KNOWLEDGE AND CONCERN:

	Security and safety for all the digital devices used by you	Security and safety for all the digital devices used by your family members	Password security	Antivirus software	The operating system security settings.	Internet browser security settings.	The backup configuration settings.	The applications security and management in your digital devices.	The security configuration settings of the access points (modem).	Parental controls settings.
Pearson Correlation	.104	.095	.089	.130	.062	.090	.055	.027	.004	.051
Sig. (2-tailed)	.031	.048	.064	.007	.199	.062	.255	.569	.941	.294
N	434	434	434	434	434	434	434	434	434	434
Pearson Correlation	.148	.102	.130	.123	.079	.105	.094	.094	.077	.092
Sig. (2-tailed)	.002	.033	.007	.011	.099	.028	.051	.051	.110	.057
N	434	434	434	434	434	434	434	434	434	434
Pearson Correlation	.075	.094	.139	.087	.084	.097	.025	.028	.034	.013
Sig. (2-tailed)	.120	.051	.004	.071	.080	.043	.610	.565	.486	.791
N	434	434	434	434	434	434	434	434	434	434
Pearson Correlation	.042	.081	.050	.115	.070	.049	.002	.005	.013	.024
Sig. (2-tailed)	.384	.093	.302	.017	.144	.309	.973	.920	.782	.611
N	434	434	434	434	434	434	434	434	434	434
Pearson Correlation	.151	.183	.138	.196	.172	.180	.108	.137	.158	.105
Sig. (2-tailed)	.002	.000	.004	.000	.000	.000	.024	.004	.001	.029

N	434	434	434	434	434	434	434	434	434	434
Pearson Correlation	.138	.133	.133	.182	.147	.225	.118	.110	.094	.070
Sig. (2-tailed)	.004	.005	.006	.000	.002	.000	.014	.022	.051	.144
N	434	434	434	434	434	434	434	434	434	434
Pearson Correlation	.089	.124	.073	.102	.102	.094	.137	.061	.070	.040
Sig. (2-tailed)	.064	.010	.131	.034	.033	.049	.004	.206	.143	.411
N	434	434	434	434	434	434	434	434	434	434
Pearson Correlation	.108	.136	.062	.105	.098	.112	.089	.085	.087	.039
Sig. (2-tailed)	.024	.004	.200	.028	.041	.020	.064	.076	.072	.421
N	434	434	434	434	434	434	434	434	434	434
Pearson Correlation	.191	.192	.136	.179	.168	.198	.112	.164	.190	.168
Sig. (2-tailed)	.000	.000	.004	.000	.000	.000	.019	.001	.000	.000
N	434	434	434	434	434	434	434	434	434	434
Pearson Correlation	.102	.176	.079	.086	.111	.111	.053	.095	.123	.275
Sig. (2-tailed)	.033	.000	.101	.073	.020	.021	.274	.049	.010	.000
N	434	434	434	434	434	434	434	434	434	434

Knowledge and management

	Security and safety for all the digital devices used by you	Security and safety for all the digital devices used by your family members	Password security settings.	Antivirus software settings.	The operating system security settings.	The Internet browser security settings.	The backup configuration settings.	The applications security and management in your digital devices.	The security configuration settings of the access points (modem).	Parental control settings.

Pearson Correlation	.550	.425	.408	.433	.473	.468	.388	.469	.401	.370
Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
N	434	434	434	434	434	434	434	434	434	434
Pearson Correlation	.438	.586	.394	.374	.426	.395	.388	.431	.389	.454
Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
N	434	434	434	434	434	434	434	434	434	434
Pearson Correlation	.484	.382	.525	.389	.454	.401	.348	.424	.362	.334
Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
N	434	434	434	434	434	434	434	434	434	434
Pearson Correlation	.486	.398	.455	.642	.557	.515	.419	.478	.417	.407
Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
N	434	434	434	434	434	434	434	434	434	434
Pearson Correlation	.505	.403	.473	.530	.637	.568	.446	.587	.488	.446
Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
N	434	434	434	434	434	434	434	434	434	434
Pearson Correlation	.512	.449	.517	.499	.576	.583	.483	.587	.539	.421
Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
N	434	434	434	434	434	434	434	434	434	434
Pearson Correlation	.384	.366	.393	.408	.458	.464	.540	.503	.451	.358
Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
N	434	434	434	434	434	434	434	434	434	434
Pearson Correlation	.491	.417	.438	.437	.519	.508	.443	.588	.478	.400
Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
N	434	434	434	434	434	434	434	434	434	434

Pearson Correlation	.475	.451	.472	.475	.542	.526	.464	.534	.648	.447
Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
N	434	434	434	434	434	434	434	434	434	434
Pearson Correlation	.393	.485	.356	.404	.472	.456	.405	.419	.447	.664
Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000

Concern and management:

	Security and safety for all the digital devices used by you	Security and safety for all the digital devices used by your family members	Password security settings.	Antivirus software settings.	The operating system security settings	The Internet browser security settings.	The backup configuration settings.	The applications security and management in your digital devices.	The security configuration settings of the access points (modem)	Parental control settings.
Pearson Correlation	.091	.092	.099	.127	.134	.173	.095	.084	.129	.083
Sig. (2-tailed)	.059	.056	.039	.008	.005	.000	.047	.081	.007	.084
N	434	434	434	434	434	434	434	434	434	434
Pearson Correlation	.086	.130	.057	.075	.131	.102	.114	.072	.145	.205
Sig. (2-tailed)	.073	.007	.238	.117	.006	.033	.017	.136	.003	.000
N	434	434	434	434	434	434	434	434	434	434
Pearson Correlation	.070	.122	.074	.096	.102	.111	.081	.082	.109	.057
Sig. (2-tailed)	.146	.011	.122	.046	.033	.021	.093	.087	.023	.234
N	434	434	434	434	434	434	434	434	434	434
Pearson Correlation	.049	.045	.057	.045	.094	.068	.068	.054	.136	.063

Sig. (2-tailed)	.306	.354	.238	.350	.050	.158	.156	.258	.005	.190
N	434	434	434	434	434	434	434	434	434	434
Pearson Correlation	.049	.070	.031	.032	.108	.091	.074	.048	.142	.100
Sig. (2-tailed)	.305	.144	.519	.504	.024	.059	.123	.321	.003	.037
N	434	434	434	434	434	434	434	434	434	434
Pearson Correlation	.045	.075	.059	.053	.125	.156	.073	.085	.168	.077
Sig. (2-tailed)	.354	.119	.223	.272	.009	.001	.129	.076	.000	.111
N	434	434	434	434	434	434	434	434	434	434
Pearson Correlation	.070	.086	.038	.022	.050	.063	.114	.084	.065	.075
Sig. (2-tailed)	.144	.075	.430	.642	.302	.189	.018	.082	.177	.120
N	434	434	434	434	434	434	434	434	434	434
Pearson Correlation	-.023	.072	-.015	.006	.027	.076	.010	.056	.121	.060
Sig. (2-tailed)	.634	.134	.749	.894	.574	.116	.831	.241	.011	.216
N	434	434	434	434	434	434	434	434	434	434
Pearson Correlation	-.002	.042	.047	.049	.133	.115	.058	.083	.214	.061
Sig. (2-tailed)	.969	.387	.331	.306	.006	.017	.226	.085	.000	.204
N	434	434	434	434	434	434	434	434	434	434
Pearson Correlation	.039	.060	-.013	.038	.087	.069	.051	.055	.163	.274
Sig. (2-tailed)	.423	.214	.785	.435	.069	.153	.292	.250	.001	.000
N	434	434	434	434	434	434	434	434	434	434

Age:

Oneway ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Concern: Security and safety for all the digital devices used by you	Between Groups	7.595	5	1.519	1.121	.348
	Within Groups	579.900	428	1.355		
	Total	587.495	433			
Concern: Security and safety for all the digital devices used by your family members	Between Groups	3.755	5	.751	.548	.740
	Within Groups	586.743	428	1.371		
	Total	590.498	433			
Concern: Password security settings.	Between Groups	7.552	5	1.510	.779	.565
	Within Groups	829.573	428	1.938		
	Total	837.124	433			
Concern: Antivirus software settings.	Between Groups	11.545	5	2.309	1.323	.253
	Within Groups	747.146	428	1.746		
	Total	758.691	433			
Concern: The operating system security settings	Between Groups	18.402	5	3.680	2.127	.061
	Within Groups	740.483	428	1.730		
	Total	758.885	433			
Concern: The Internet browser security settings.	Between Groups	3.796	5	.759	.463	.804
	Within Groups	701.413	428	1.639		
	Total	705.210	433			
Concern: The backup configuration settings.	Between Groups	6.608	5	1.322	.752	.585
	Within Groups	752.231	428	1.758		
	Total	758.839	433			
Concern: The applications security and management in your digital devices.	Between Groups	12.467	5	2.493	1.451	.205
	Within Groups	735.560	428	1.719		
	Total	748.028	433			
Concern: The security configuration settings of the access points (modem)	Between Groups	14.490	5	2.898	1.598	.159
	Within Groups	775.936	428	1.813		
	Total	790.426	433			
Concern: Parental control settings.	Between Groups	52.867	5	10.573	5.004	.000
	Within Groups	904.386	428	2.113		
	Total	957.253	433			

Oneway ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Knowledge: Security and safety for all the digital devices used by you	Between Groups	4.769	5	.954	.792	.556
	Within Groups	515.270	428	1.204		
	Total	520.039	433			
Knowledge: Security and safety for all the digital devices used by your family members	Between Groups	19.711	5	3.942	2.928	.013
	Within Groups	576.319	428	1.347		
	Total	596.030	433			
Knowledge: Password security settings.	Between Groups	3.926	5	.785	.642	.668
	Within Groups	523.459	428	1.223		
	Total	527.385	433			
Knowledge: Antivirus software settings.	Between Groups	15.057	5	3.011	1.881	.096
	Within Groups	685.148	428	1.601		
	Total	700.205	433			
Knowledge: The operating system security settings.	Between Groups	3.378	5	.676	.435	.824
	Within Groups	664.504	428	1.553		
	Total	667.882	433			
Knowledge: The Internet browser security settings.	Between Groups	3.833	5	.767	.554	.735
	Within Groups	592.001	428	1.383		
	Total	595.834	433			
Knowledge: The backup configuration settings.	Between Groups	8.077	5	1.615	1.047	.389
	Within Groups	660.294	428	1.543		
	Total	668.371	433			
Knowledge: The applications security and management in your digital devices.	Between Groups	7.727	5	1.545	1.019	.406
	Within Groups	649.157	428	1.517		
	Total	656.885	433			
Knowledge: The security configuration settings of the access points (modem).	Between Groups	16.640	5	3.328	1.981	.080
	Within Groups	719.214	428	1.680		
	Total	735.855	433			
Knowledge: Parental controls settings.	Between Groups	10.295	5	2.059	1.329	.251
	Within Groups	663.164	428	1.549		
	Total	673.459	433			

Oneway ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
management: Security and safety for all the digital devices used by you	Between Groups	3.006	5	.601	.465	.802
	Within Groups	553.473	428	1.293		
	Total	556.479	433			
management: Security and safety for all the digital devices used by your family members	Between Groups	22.036	5	4.407	3.199	.008
	Within Groups	589.605	428	1.378		
	Total	611.641	433			
management: Password security settings.	Between Groups	6.129	5	1.226	.905	.477
	Within Groups	579.410	428	1.354		
	Total	585.539	433			
management: Antivirus software settings.	Between Groups	6.203	5	1.241	.787	.559
	Within Groups	674.369	428	1.576		
	Total	680.571	433			
management: The operating system security settings.	Between Groups	4.060	5	.812	.545	.742
	Within Groups	638.051	428	1.491		
	Total	642.111	433			
management: The Internet browser security settings.	Between Groups	3.689	5	.738	.463	.804
	Within Groups	682.682	428	1.595		
	Total	686.371	433			
management: The backup configuration settings.	Between Groups	4.628	5	.926	.602	.698
	Within Groups	657.549	428	1.536		
	Total	662.177	433			
management: The applications security and management in your digital devices.	Between Groups	7.355	5	1.471	.971	.435
	Within Groups	648.104	428	1.514		
	Total	655.459	433			
management: The security configuration settings of the access points (modem).	Between Groups	10.087	5	2.017	1.140	.338
	Within Groups	757.461	428	1.770		
	Total	767.548	433			
	Between Groups	32.556	5	6.511	3.833	.002
	Within Groups	726.993	428	1.699		

management: Parental control settings.	Total	759.548	433			

Oneway ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Ease: Security and safety for all the digital devices used by you.	Between Groups	13.809	5	2.762	2.861	.015
	Within Groups	401.540	416	.965		
	Total	415.348	421			
Ease: Security and safety for all the digital devices used by your family members.	Between Groups	7.029	5	1.406	1.430	.212
	Within Groups	381.319	388	.983		
	Total	388.348	393			
Ease: Password security settings.	Between Groups	9.979	5	1.996	1.726	.127
	Within Groups	478.733	414	1.156		
	Total	488.712	419			
Ease: Antivirus software settings.	Between Groups	4.228	5	.846	.725	.605
	Within Groups	459.750	394	1.167		
	Total	463.977	399			
Ease: The operating system security settings.	Between Groups	11.098	5	2.220	1.842	.104
	Within Groups	471.275	391	1.205		
	Total	482.373	396			
Ease: The Internet browser security settings.	Between Groups	13.404	5	2.681	2.300	.044
	Within Groups	452.180	388	1.165		
	Total	465.584	393			
Ease:The backup configuration settings.	Between Groups	19.182	5	3.836	3.299	.006
	Within Groups	443.025	381	1.163		
	Total	462.207	386			
Ease: The applications security and management in your digital devices.	Between Groups	15.056	5	3.011	2.575	.026
	Within Groups	457.276	391	1.170		
	Total	472.332	396			
Ease: The security configuration settings of the access points (modem).	Between Groups	10.988	5	2.198	1.641	.148
	Within Groups	487.523	364	1.339		
	Total	498.511	369			
	Between Groups	6.577	5	1.315	1.157	.330

Ease: Parental control settings.	Within Groups	405.935	357	1.137		
	Total	412.512	362			

IT experience:

Oneway ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Concern: Security and safety for all the digital devices used by you	Between Groups	43.513	4	10.878	8.579	.000
	Within Groups	543.983	429	1.268		
	Total	587.495	433			
Concern: Security and safety for all the digital devices used by your family members	Between Groups	12.723	4	3.181	2.362	.053
	Within Groups	577.775	429	1.347		
	Total	590.498	433			
Concern: Password security settings.	Between Groups	34.141	4	8.535	4.560	.001
	Within Groups	802.983	429	1.872		
	Total	837.124	433			
Concern: Antivirus software settings.	Between Groups	8.661	4	2.165	1.239	.294
	Within Groups	750.030	429	1.748		
	Total	758.691	433			
Concern: The operating system security settings	Between Groups	19.382	4	4.846	2.811	.025
	Within Groups	739.502	429	1.724		
	Total	758.885	433			
Concern: The Internet browser security settings.	Between Groups	23.851	4	5.963	3.754	.005
	Within Groups	681.359	429	1.588		
	Total	705.210	433			
Concern: The backup configuration settings.	Between Groups	15.990	4	3.998	2.309	.057
	Within Groups	742.848	429	1.732		
	Total	758.839	433			
Concern: The applications security and management in your digital devices.	Between Groups	18.175	4	4.544	2.671	.032
	Within Groups	729.852	429	1.701		
	Total	748.028	433			
Concern: The security configuration settings of the access points (modem)	Between Groups	26.773	4	6.693	3.760	.005
	Within Groups	763.653	429	1.780		
	Total	790.426	433			

Concern: Parental control settings.	Between Groups	13.801	4	3.450	1.569	.182
	Within Groups	943.453	429	2.199		
	Total	957.253	433			

Oneway ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Knowledge: Security and safety for all the digital devices used by you	Between Groups	100.794	4	25.199	25.785	.000
	Within Groups	419.245	429	.977		
	Total	520.039	433			
Knowledge: Security and safety for all the digital devices used by your family members	Between Groups	89.823	4	22.456	19.031	.000
	Within Groups	506.207	429	1.180		
	Total	596.030	433			
Knowledge: Password security settings.	Between Groups	41.196	4	10.299	9.087	.000
	Within Groups	486.189	429	1.133		
	Total	527.385	433			
Knowledge: Antivirus software settings.	Between Groups	98.955	4	24.739	17.651	.000
	Within Groups	601.250	429	1.402		
	Total	700.205	433			
Knowledge: The operating system security settings.	Between Groups	81.562	4	20.391	14.919	.000
	Within Groups	586.320	429	1.367		
	Total	667.882	433			
Knowledge: The Internet browser security settings.	Between Groups	83.522	4	20.880	17.485	.000
	Within Groups	512.313	429	1.194		
	Total	595.834	433			
Knowledge: The backup configuration settings.	Between Groups	84.779	4	21.195	15.580	.000
	Within Groups	583.592	429	1.360		
	Total	668.371	433			
Knowledge: The applications security and management in your digital devices.	Between Groups	86.913	4	21.728	16.354	.000
	Within Groups	569.972	429	1.329		
	Total	656.885	433			
Knowledge: The security configuration settings of the access points (modem).	Between Groups	110.027	4	27.507	18.856	.000
	Within Groups	625.827	429	1.459		
	Total	735.855	433			

Knowledge: Parental controls settings.	Between Groups	63.044	4	15.761	11.077	.000
	Within Groups	610.415	429	1.423		
	Total	673.459	433			

Oneway ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
management: Security and safety for all the digital devices used by you	Between Groups	41.717	4	10.429	8.692	.000
	Within Groups	514.763	429	1.200		
	Total	556.479	433			
management: Security and safety for all the digital devices used by your family members	Between Groups	42.135	4	10.534	7.935	.000
	Within Groups	569.505	429	1.328		
	Total	611.641	433			
management: Password security settings.	Between Groups	36.651	4	9.163	7.161	.000
	Within Groups	548.888	429	1.279		
	Total	585.539	433			
management: Antivirus software settings.	Between Groups	49.332	4	12.333	8.382	.000
	Within Groups	631.240	429	1.471		
	Total	680.571	433			
management: The operating system security settings.	Between Groups	50.510	4	12.628	9.157	.000
	Within Groups	591.601	429	1.379		
	Total	642.111	433			
management: The Internet browser security settings.	Between Groups	52.847	4	13.212	8.946	.000
	Within Groups	633.524	429	1.477		
	Total	686.371	433			
management: The backup configuration settings.	Between Groups	47.796	4	11.949	8.344	.000
	Within Groups	614.382	429	1.432		
	Total	662.177	433			
management: The applications security and management in your digital devices.	Between Groups	41.749	4	10.437	7.296	.000
	Within Groups	613.710	429	1.431		
	Total	655.459	433			
management: The security configuration settings of	Between Groups	47.236	4	11.809	7.033	.000
	Within Groups	720.313	429	1.679		

the access points (modem).	Total	767.548	433			
management: Parental control settings.	Between Groups	51.946	4	12.986	7.873	.000
	Within Groups	707.602	429	1.649		
	Total	759.548	433			

Oneway ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Ease: Security and safety for all the digital devices used by you.	Between Groups	15.864	4	3.966	4.140	.003
	Within Groups	399.484	417	.958		
	Total	415.348	421			
Ease: Security and safety for all the digital devices used by your family members.	Between Groups	13.389	4	3.347	3.472	.008
	Within Groups	374.959	389	.964		
	Total	388.348	393			
Ease: Password security settings.	Between Groups	2.296	4	.574	.490	.743
	Within Groups	486.416	415	1.172		
	Total	488.712	419			
Ease: Antivirus software settings.	Between Groups	21.020	4	5.255	4.686	.001
	Within Groups	442.958	395	1.121		
	Total	463.977	399			
Ease: The operating system security settings.	Between Groups	13.529	4	3.382	2.828	.025
	Within Groups	468.844	392	1.196		
	Total	482.373	396			
Ease: The Internet browser security settings.	Between Groups	36.144	4	9.036	8.185	.000
	Within Groups	429.439	389	1.104		
	Total	465.584	393			
Ease:The backup configuration settings.	Between Groups	13.437	4	3.359	2.860	.023
	Within Groups	448.769	382	1.175		
	Total	462.207	386			
Ease: The applications security and management in your digital devices.	Between Groups	10.745	4	2.686	2.281	.060
	Within Groups	461.588	392	1.178		
	Total	472.332	396			
Ease: The security configuration settings of	Between Groups	11.157	4	2.789	2.089	.082
	Within Groups	487.354	365	1.335		

the access points (modem).	Total	498.511	369			
Ease: Parental control settings.	Between Groups	7.363	4	1.841	1.627	.167
	Within Groups	405.149	358	1.132		
	Total	412.512	362			

Education:

Oneway ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Concern: Security and safety for all the digital devices used by you	Between Groups	11.699	4	2.925	2.179	.070
	Within Groups	575.796	429	1.342		
	Total	587.495	433			
Concern: Security and safety for all the digital devices used by your family members	Between Groups	1.967	4	.492	.358	.838
	Within Groups	588.531	429	1.372		
	Total	590.498	433			
Concern: Password security settings.	Between Groups	18.063	4	4.516	2.365	.052
	Within Groups	819.061	429	1.909		
	Total	837.124	433			
Concern: Antivirus software settings.	Between Groups	18.253	4	4.563	2.644	.033
	Within Groups	740.438	429	1.726		
	Total	758.691	433			
Concern: The operating system security settings	Between Groups	23.316	4	5.829	3.400	.009
	Within Groups	735.568	429	1.715		
	Total	758.885	433			
Concern: The Internet browser security settings.	Between Groups	7.210	4	1.803	1.108	.352
	Within Groups	698.000	429	1.627		
	Total	705.210	433			
Concern: The backup configuration settings.	Between Groups	8.252	4	2.063	1.179	.319
	Within Groups	750.587	429	1.750		
	Total	758.839	433			
Concern: The applications security and management in your digital devices.	Between Groups	7.807	4	1.952	1.131	.341
	Within Groups	740.220	429	1.725		
	Total	748.028	433			
Concern: The security configuration settings of the access points (modem)	Between Groups	12.438	4	3.109	1.715	.146
	Within Groups	777.988	429	1.813		
	Total	790.426	433			

Concern: Parental control settings.	Between Groups	22.097	4	5.524	2.534	.040
	Within Groups	935.157	429	2.180		
	Total	957.253	433			

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Knowledge: Security and safety for all the digital devices used by you	Between Groups	4.146	4	1.036	.862	.487
	Within Groups	515.893	429	1.203		
	Total	520.039	433			
Knowledge: Security and safety for all the digital devices used by your family members	Between Groups	15.490	4	3.873	2.862	.023
	Within Groups	580.540	429	1.353		
	Total	596.030	433			
Knowledge: Password security settings.	Between Groups	5.557	4	1.389	1.142	.336
	Within Groups	521.828	429	1.216		
	Total	527.385	433			
Knowledge: Antivirus software settings.	Between Groups	13.166	4	3.291	2.055	.086
	Within Groups	687.039	429	1.601		
	Total	700.205	433			
Knowledge: The operating system security settings.	Between Groups	6.596	4	1.649	1.070	.371
	Within Groups	661.286	429	1.541		
	Total	667.882	433			
Knowledge: The Internet browser security settings.	Between Groups	4.277	4	1.069	.775	.542
	Within Groups	591.557	429	1.379		
	Total	595.834	433			
Knowledge: The backup configuration settings.	Between Groups	9.214	4	2.304	1.499	.201
	Within Groups	659.157	429	1.536		
	Total	668.371	433			
Knowledge: The applications security and management in your digital devices.	Between Groups	5.670	4	1.418	.934	.444
	Within Groups	651.215	429	1.518		
	Total	656.885	433			
Knowledge: The security configuration settings of the access points (modem).	Between Groups	8.282	4	2.070	1.221	.301
	Within Groups	727.573	429	1.696		
	Total	735.855	433			
	Between Groups	9.045	4	2.261	1.460	.213

Knowledge: Parental controls settings.	Within Groups	664.414	429	1.549		
	Total	673.459	433			

Oneway ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
management: Security and safety for all the digital devices used by you	Between Groups	2.746	4	.687	.532	.712
	Within Groups	553.733	429	1.291		
	Total	556.479	433			
management: Security and safety for all the digital devices used by your family members	Between Groups	3.307	4	.827	.583	.675
	Within Groups	608.333	429	1.418		
	Total	611.641	433			
management: Password security settings.	Between Groups	8.529	4	2.132	1.585	.177
	Within Groups	577.010	429	1.345		
	Total	585.539	433			
management: Antivirus software settings.	Between Groups	4.820	4	1.205	.765	.548
	Within Groups	675.751	429	1.575		
	Total	680.571	433			
management: The operating system security settings.	Between Groups	4.724	4	1.181	.795	.529
	Within Groups	637.386	429	1.486		
	Total	642.111	433			
management: The Internet browser security settings.	Between Groups	4.777	4	1.194	.752	.557
	Within Groups	681.594	429	1.589		
	Total	686.371	433			
management: The backup configuration settings.	Between Groups	11.316	4	2.829	1.865	.116
	Within Groups	650.861	429	1.517		
	Total	662.177	433			
management: The applications security	Between Groups	10.031	4	2.508	1.667	.157
	Within Groups	645.427	429	1.504		

and management in your digital devices.	Total	655.459	433			
management: The security configuration settings of the access points (modem).	Between Groups	4.262	4	1.066	.599	.664
	Within Groups	763.286	429	1.779		
	Total	767.548	433			
management: Parental control settings.	Between Groups	10.962	4	2.740	1.571	.181
	Within Groups	748.586	429	1.745		
	Total	759.548	433			

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Ease: Security and safety for all the digital devices used by you.	Between Groups	6.758	4	1.689	1.724	.144
	Within Groups	408.591	417	.980		
	Total	415.348	421			
Ease: Security and safety for all the digital devices used by your family members.	Between Groups	1.784	4	.446	.449	.773
	Within Groups	386.564	389	.994		
	Total	388.348	393			
Ease: Password security settings.	Between Groups	8.949	4	2.237	1.935	.104
	Within Groups	479.763	415	1.156		
	Total	488.712	419			
Ease: Antivirus software settings.	Between Groups	14.384	4	3.596	3.159	.014
	Within Groups	449.593	395	1.138		
	Total	463.977	399			
Ease: The operating system security settings.	Between Groups	3.866	4	.967	.792	.531
	Within Groups	478.506	392	1.221		
	Total	482.373	396			
Ease: The Internet browser security settings.	Between Groups	4.186	4	1.047	.882	.474
	Within Groups	461.398	389	1.186		
	Total	465.584	393			
Ease:The backup configuration settings.	Between Groups	15.825	4	3.956	3.386	.010
	Within Groups	446.382	382	1.169		
	Total	462.207	386			
Ease: The applications security	Between Groups	5.395	4	1.349	1.132	.341
	Within Groups	466.937	392	1.191		

and management in your digital devices.	Total	472.332	396			
Ease: The security configuration settings of the access points (modem).	Between Groups	15.102	4	3.776	2.851	.024
	Within Groups	483.408	365	1.324		
	Total	498.511	369			
Ease: Parental control settings.	Between Groups	7.394	4	1.849	1.634	.165
	Within Groups	405.118	358	1.132		
	Total	412.512	362			

IT experience and agree

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Agree: Different level of security settings should be applied to all the digital devices. (such as low, medium and high level)	Between Groups	2.738	4	.684	.710	.586
	Within Groups	413.818	429	.965		
	Total	416.555	433			
Agree: Different security settings should be implemented and focused upon the user rather than the device	Between Groups	5.714	4	1.429	1.136	.339
	Within Groups	539.670	429	1.258		
	Total	545.385	433			
Agree: One security level should be applied on all the devices belongs to one user?	Between Groups	.976	4	.244	.151	.962
	Within Groups	690.941	429	1.611		
	Total	691.917	433			
Agree: It would be a good idea to have pre-defined templates of security settings	Between Groups	5.587	4	1.397	1.354	.249
	Within Groups	442.404	429	1.031		
	Total	447.991	433			

Agree: Different level of security settings should be applied to all the digital devices. (such as low, medium and high level)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	13	3.0	3.0	3.0
	2	14	3.2	3.2	6.2
	3	49	11.3	11.3	17.5
	4	139	32.0	32.0	49.5
	5	219	50.5	50.5	100.0
	Total	434	100.0	100.0	

Agree: Different security settings should be implemented and focused upon the user rather than the device

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	17	3.9	3.9	3.9
	2	39	9.0	9.0	12.9
	3	95	21.9	21.9	34.8
	4	130	30.0	30.0	64.7
	5	153	35.3	35.3	100.0
	Total	434	100.0	100.0	

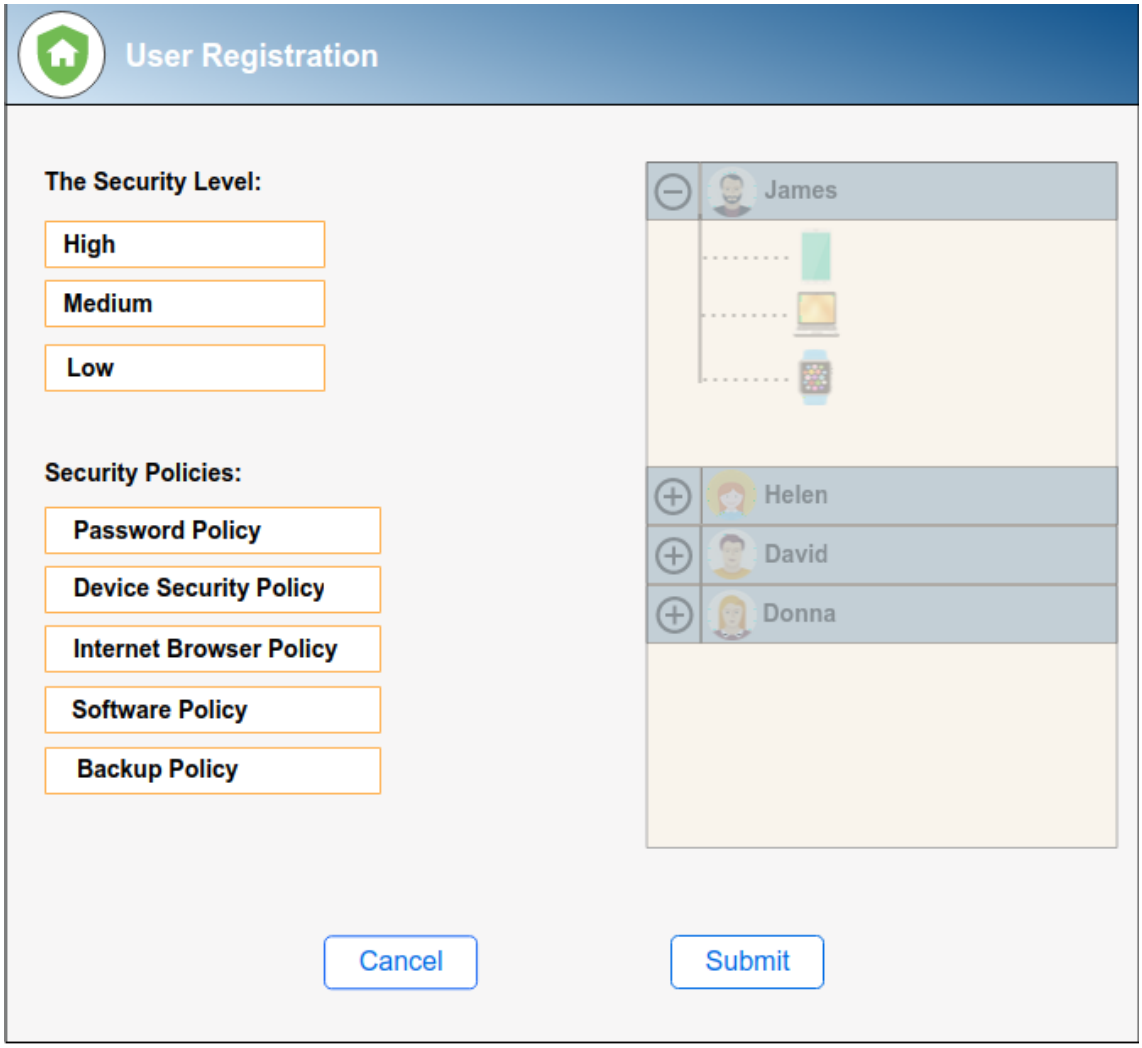
Agree: One security level should be applied on all the devices belongs to one user?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	22	5.1	5.1	5.1
	2	76	17.5	17.5	22.6
	3	61	14.1	14.1	36.6
	4	114	26.3	26.3	62.9
	5	161	37.1	37.1	100.0
	Total	434	100.0	100.0	

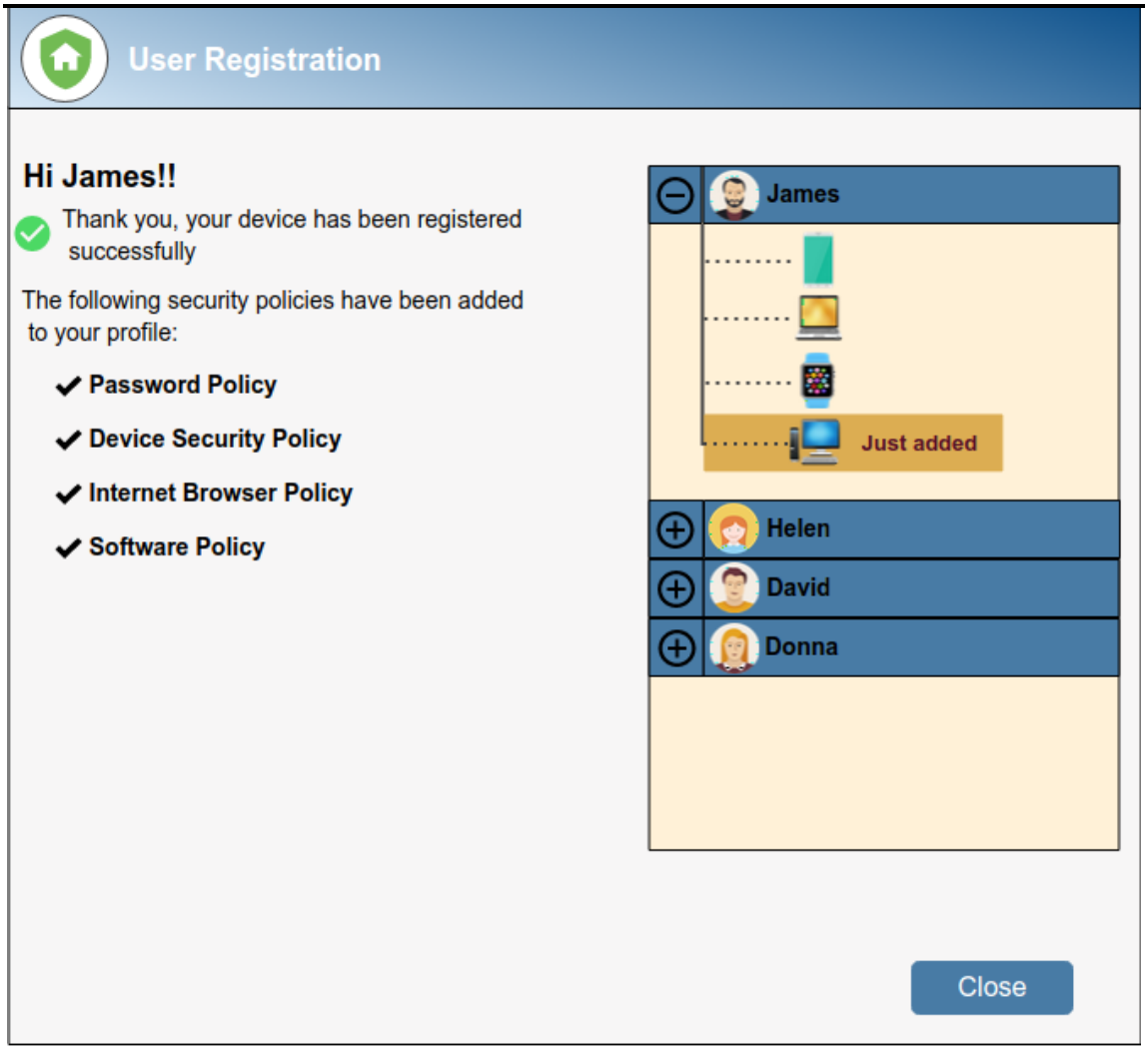
Agree: It would be a good idea to have pre-defined templates of security settings

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	14	3.2	3.2	3.2
	2	22	5.1	5.1	8.3
	3	75	17.3	17.3	25.6
	4	164	37.8	37.8	63.4
	5	159	36.6	36.6	100.0
	Total	434	100.0	100.0	

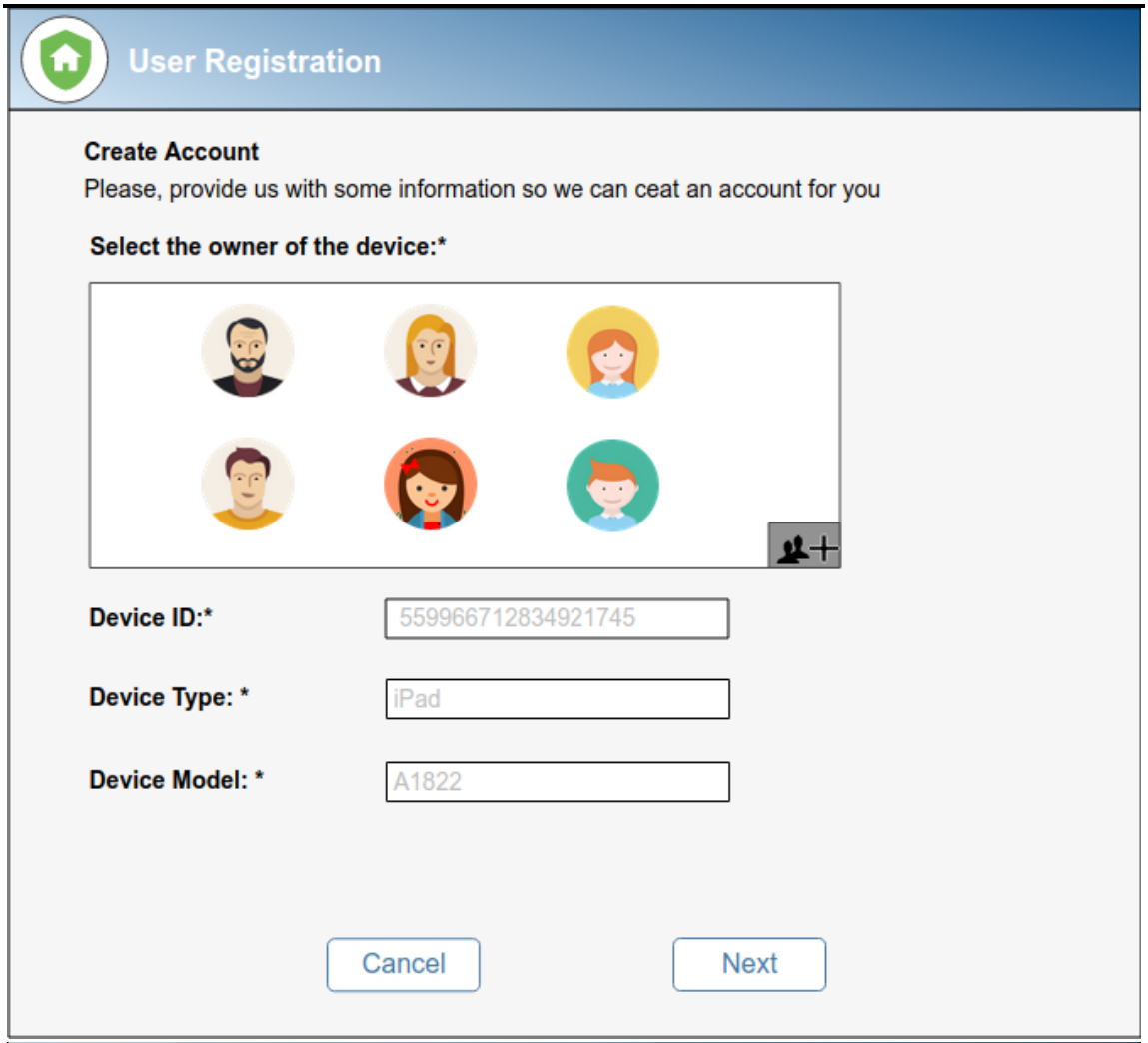
Appendix E: Mock-up Design Interfaces

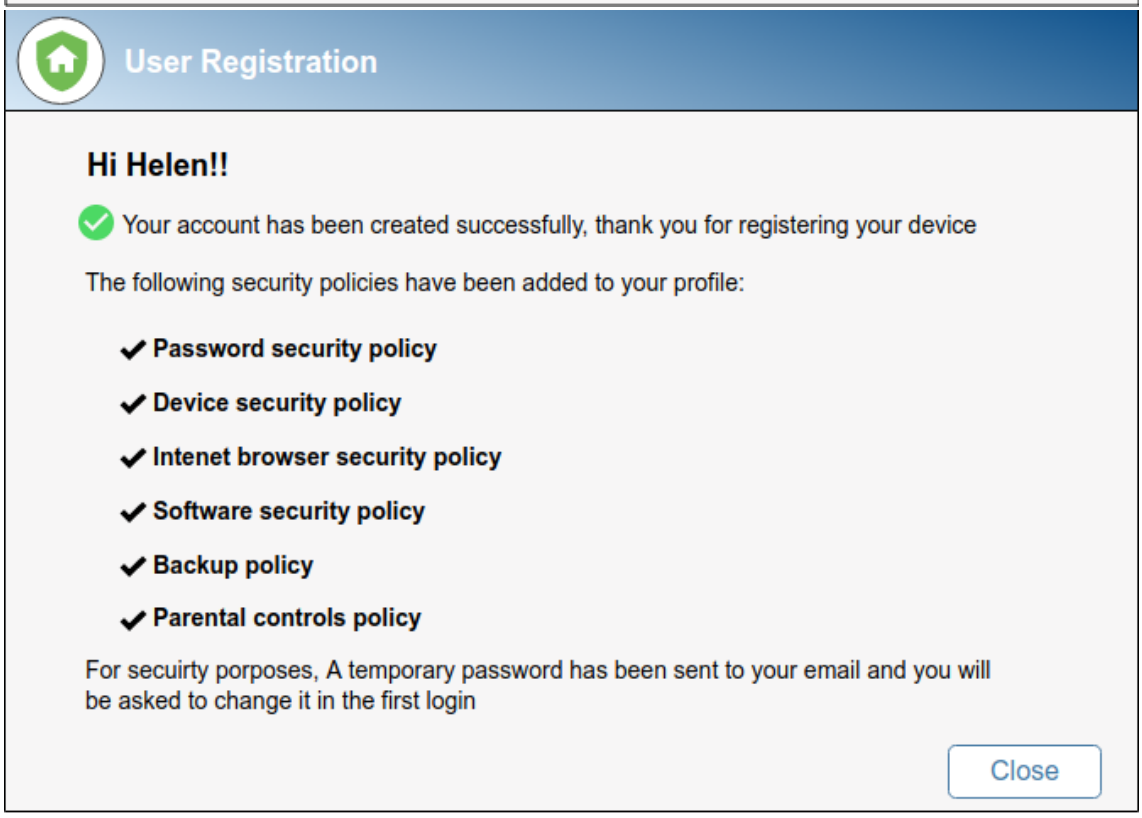



User Registration
The Security Level:
High
Medium
Low
Security Policies:
Password Policy
Device Security Policy
Internet Browser Policy
Software Policy
Backup Policy
James
Helen
David
Donna
Cancel
Submit

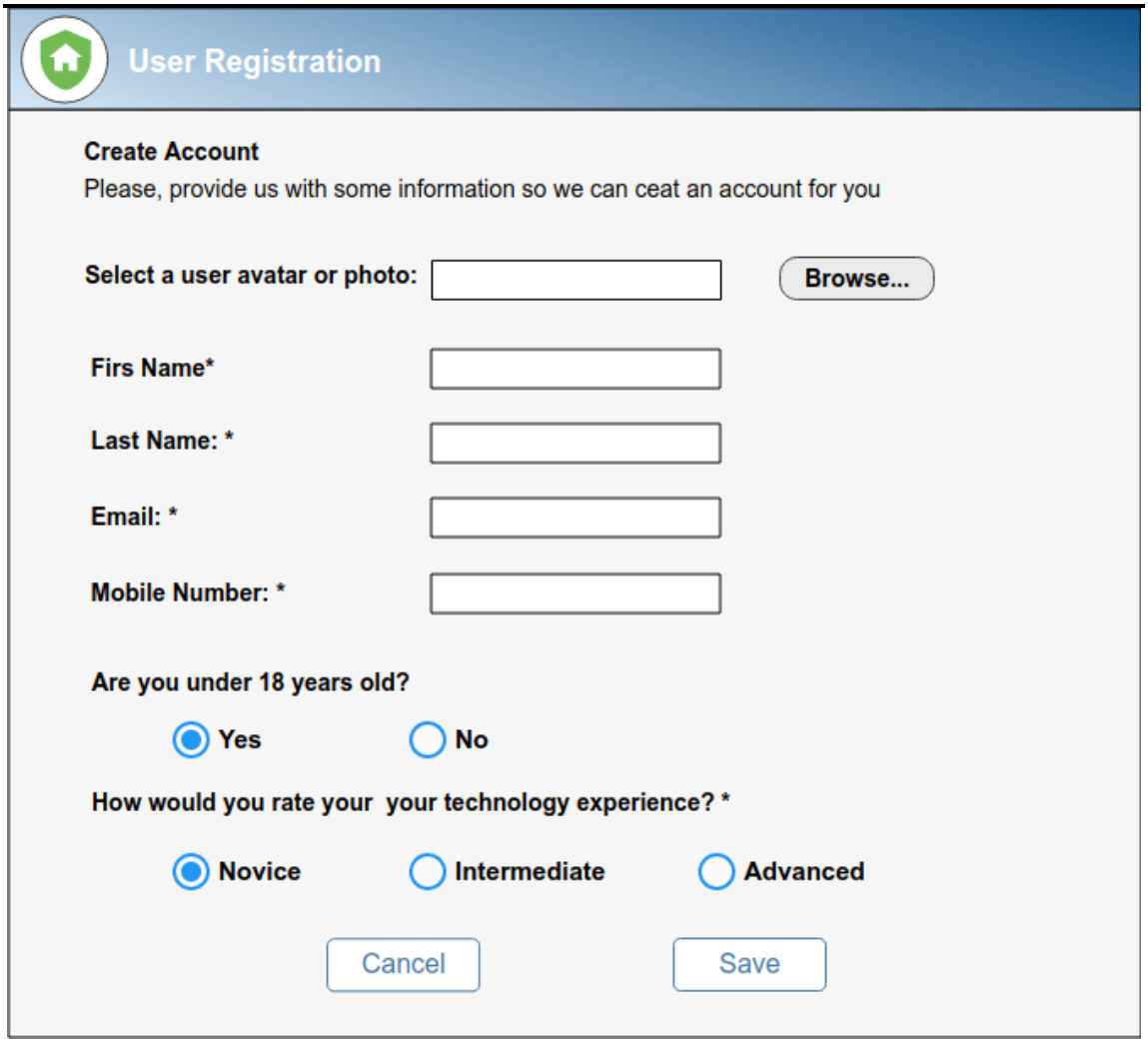

User Registration
Hi James!!
Thank you, your device has been registered successfully
The following security policies have been added to your profile:
Password Policy
Device Security Policy
Internet Browser Policy
Software Policy
James
Just added
Helen
David
Donna
Close

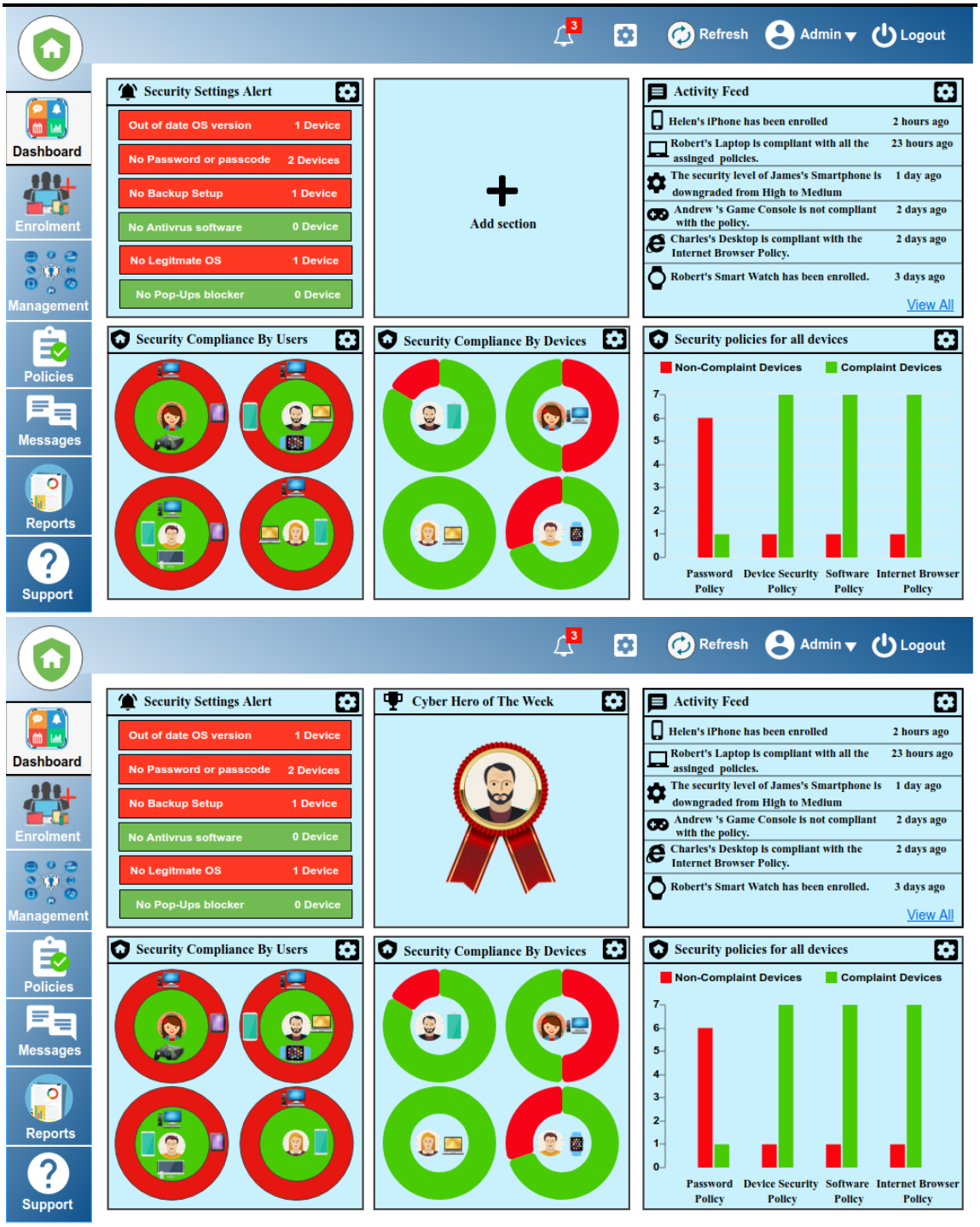

User Registration
The Security Level:
High
Medium
Low
Security Policies:
Password Policy
Device Security Policy
Internet Browser Policy
Software Policy
Backup Policy
James
Helen
David
Donna
Cancel
Submit

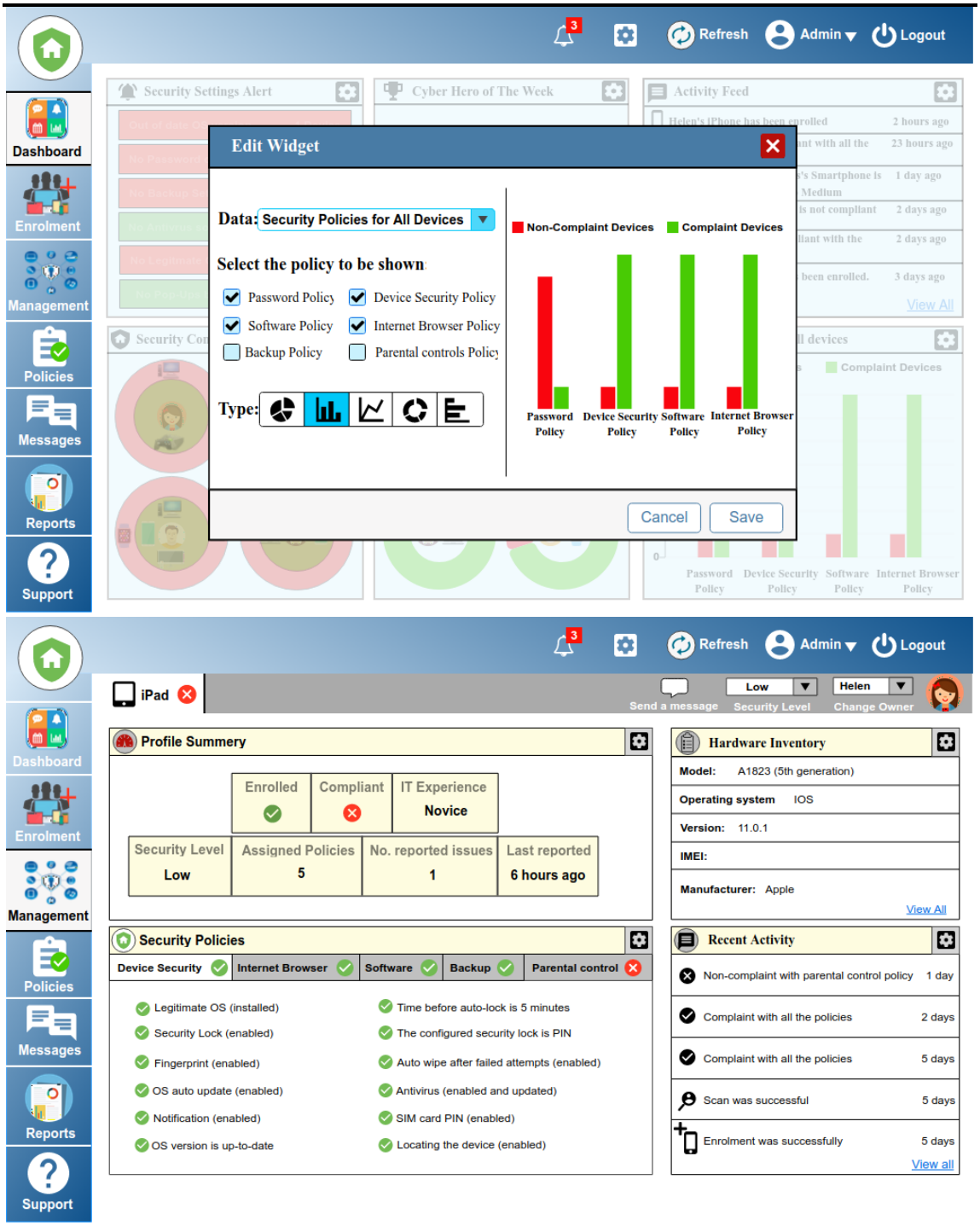

User Registration
Create Account
Please, provide us with some information so we can ceat an account for you
Select the owner of the device:*
Device ID:*
559966712834921745
Device Type: *
iPad
Device Model: *
A1822
Cancel
Next

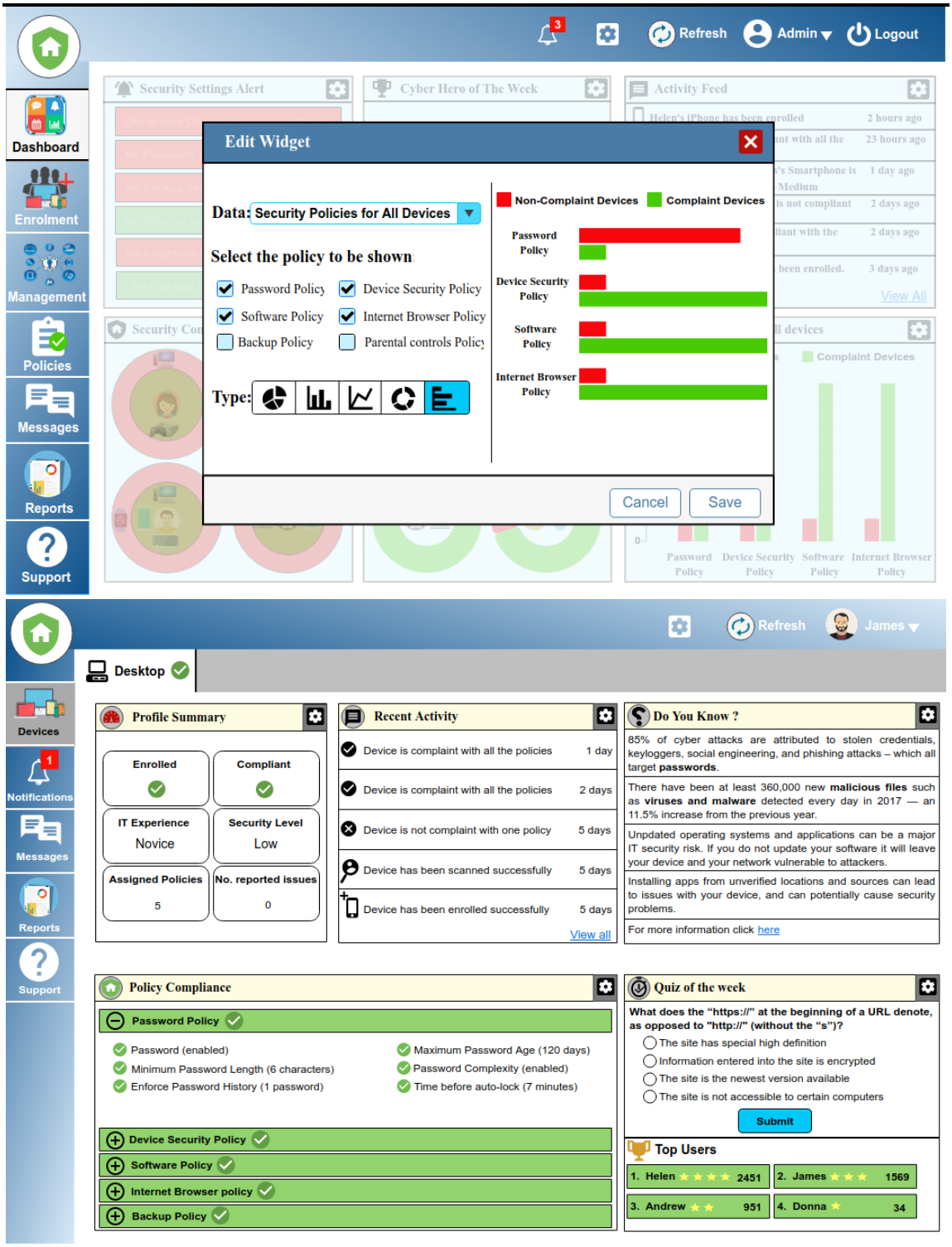

User Registration
Hi Helen!!
Your account has been created successfully, thank you for registering your device
The following security policies have been added to your profile:
Password security policy
Device security policy
Intenet browser security policy
Software security policy
Backup policy
Parental controls policy
For secuirty porposes, A temporary password has been sent to your email and you will be asked to change it in the first login
Close

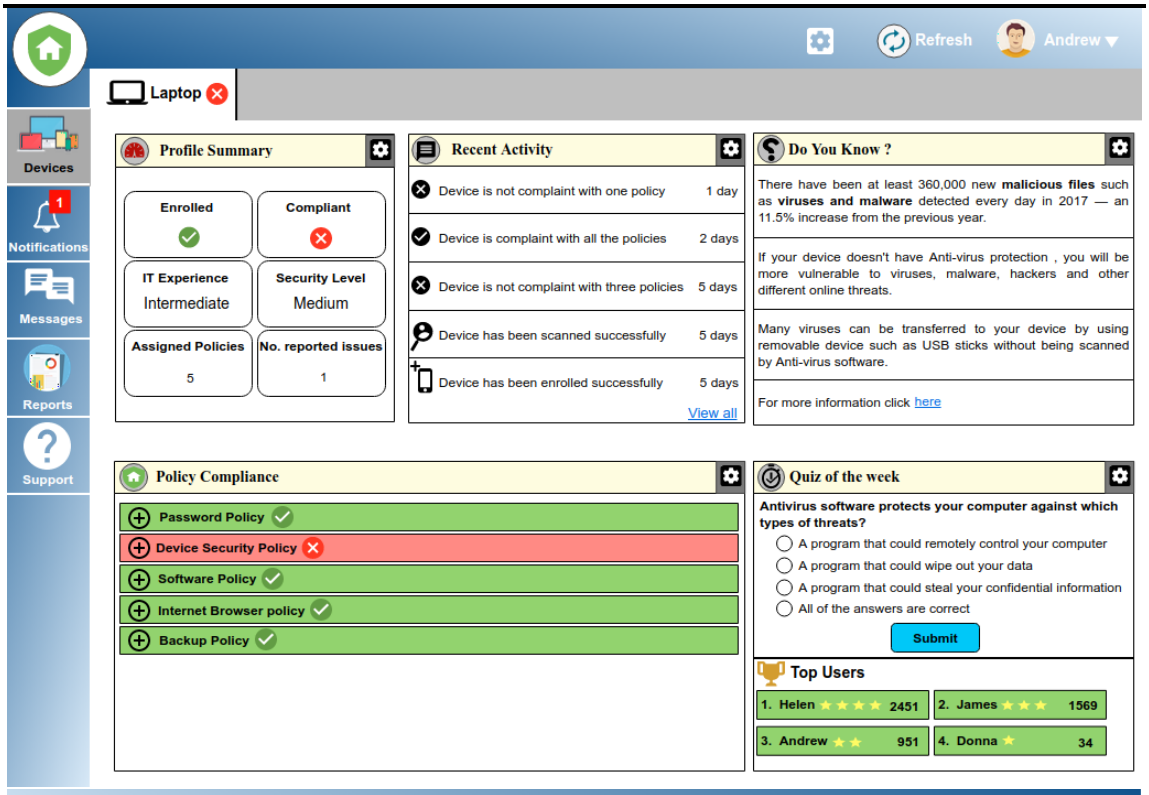

User Registration
Create Account
Please, provide us with some information so we can ceat an account for you
Select the owner of the device:*
Device ID:*
559966712834921745
Device Type: *
iPad
Device Model: *
A1822
Cancel
Next

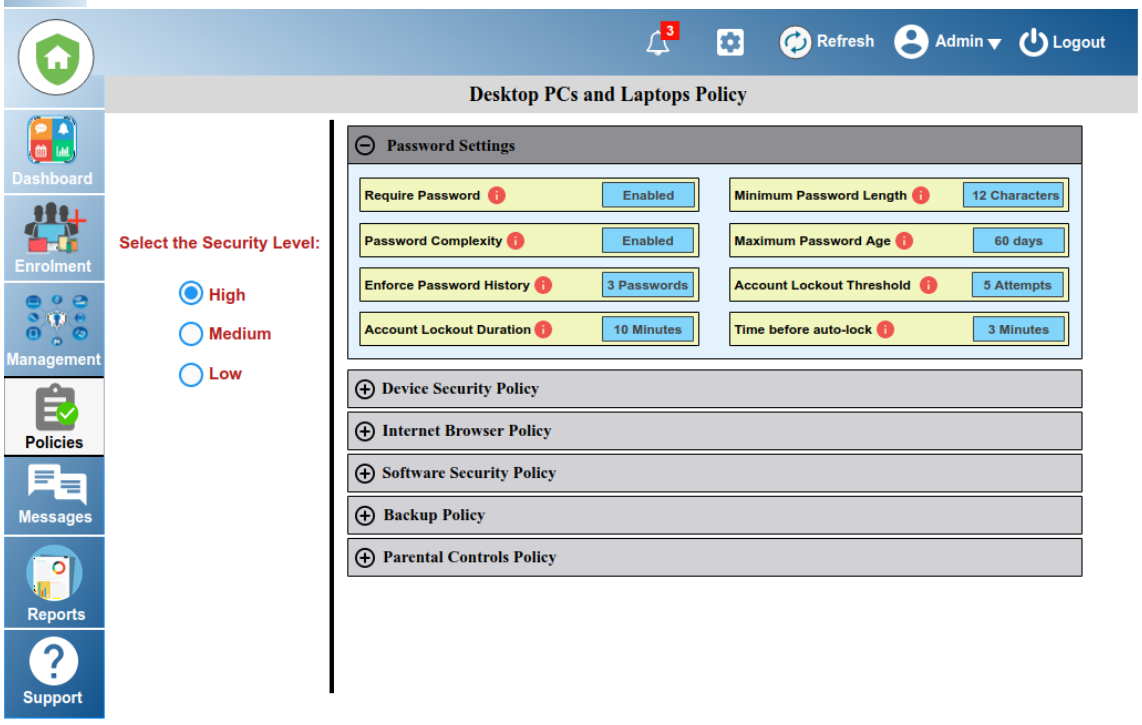

User Registration
Create Account
Please, provide us with some information so we can ceat an account for you
Select a user avatar or photo:
Browse...
Firs Name*
Last Name: *
Email: *
Mobile Number: *
Are you under 18 years old?
Yes
No
How would you rate your your technology experience? *
Novice
Intermediate
Advanced
Cancel
Save

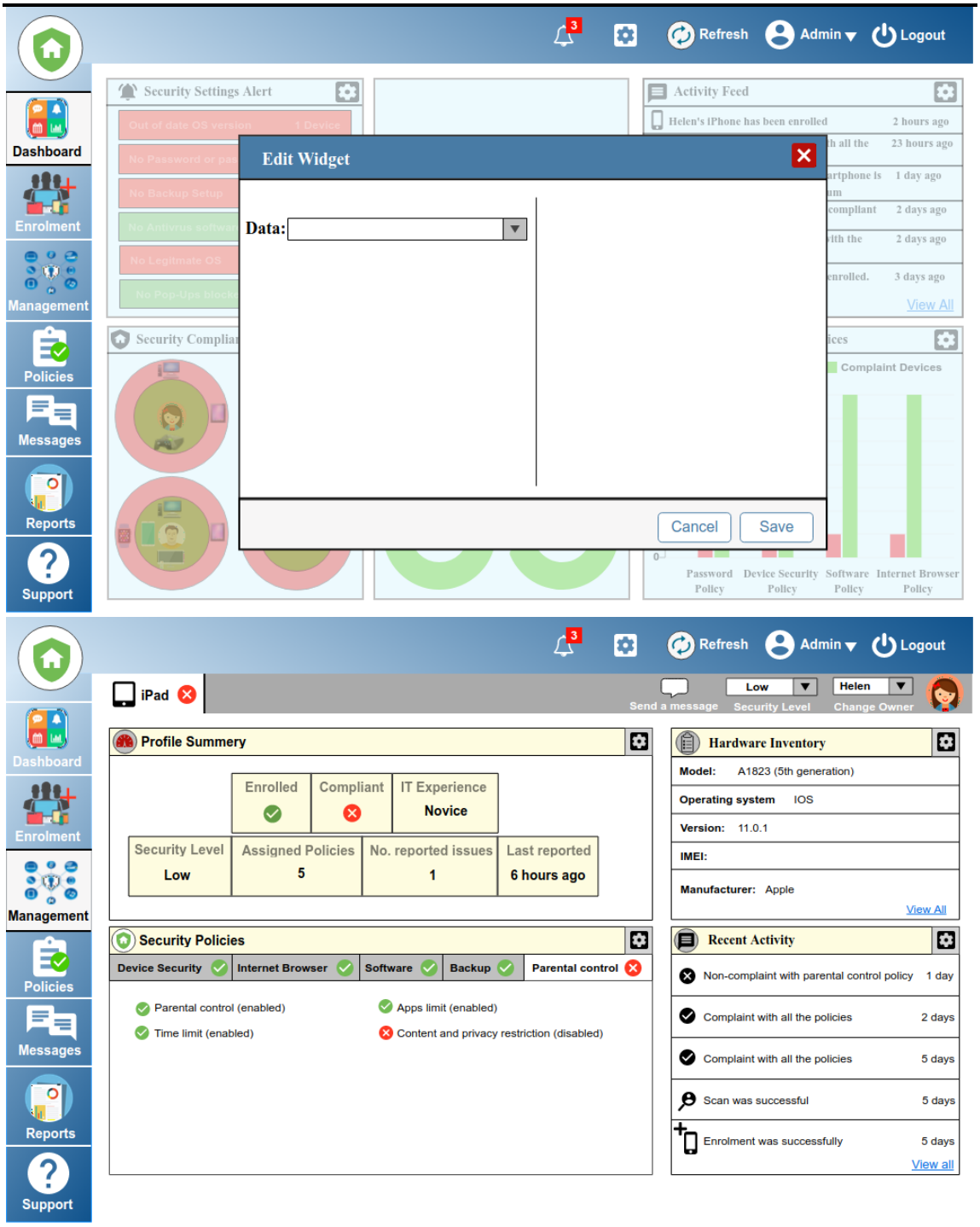

Refresh
Admin
Logout
Dashboard
Enrolment
Management
Policies
Messages
Reports
Support
Security Settings Alert
Out of date OS version 1 Device
No Password or passcode 2 Devices
No Backup Setup 1 Device
No Antivrus software 0 Device
No Legitmate OS 1 Device
No Pop-Ups blocker 0 Device
Add section
Activity Feed
Helen's iPhone has been enrolled 2 hours ago
Robert's Laptop is compliant with all the assinged policies. 23 hours ago
The security level of James's Smartphone is downgraded from High to Medium 1 day ago
Andrew 's Game Console is not compliant with the policy. 2 days ago
Charles's Desktop is compliant with the Internet Browser Policy. 2 days ago
Robert's Smart Watch has been enrolled. 3 days ago
View All
Security Compliance By Users
Security Compliance By Devices
Security policies for all devices
Non-Complaint Devices
Complaint Devices
Password Policy
Device Security Policy
Software Policy
Internet Browser Policy
Cyber Hero of The Week

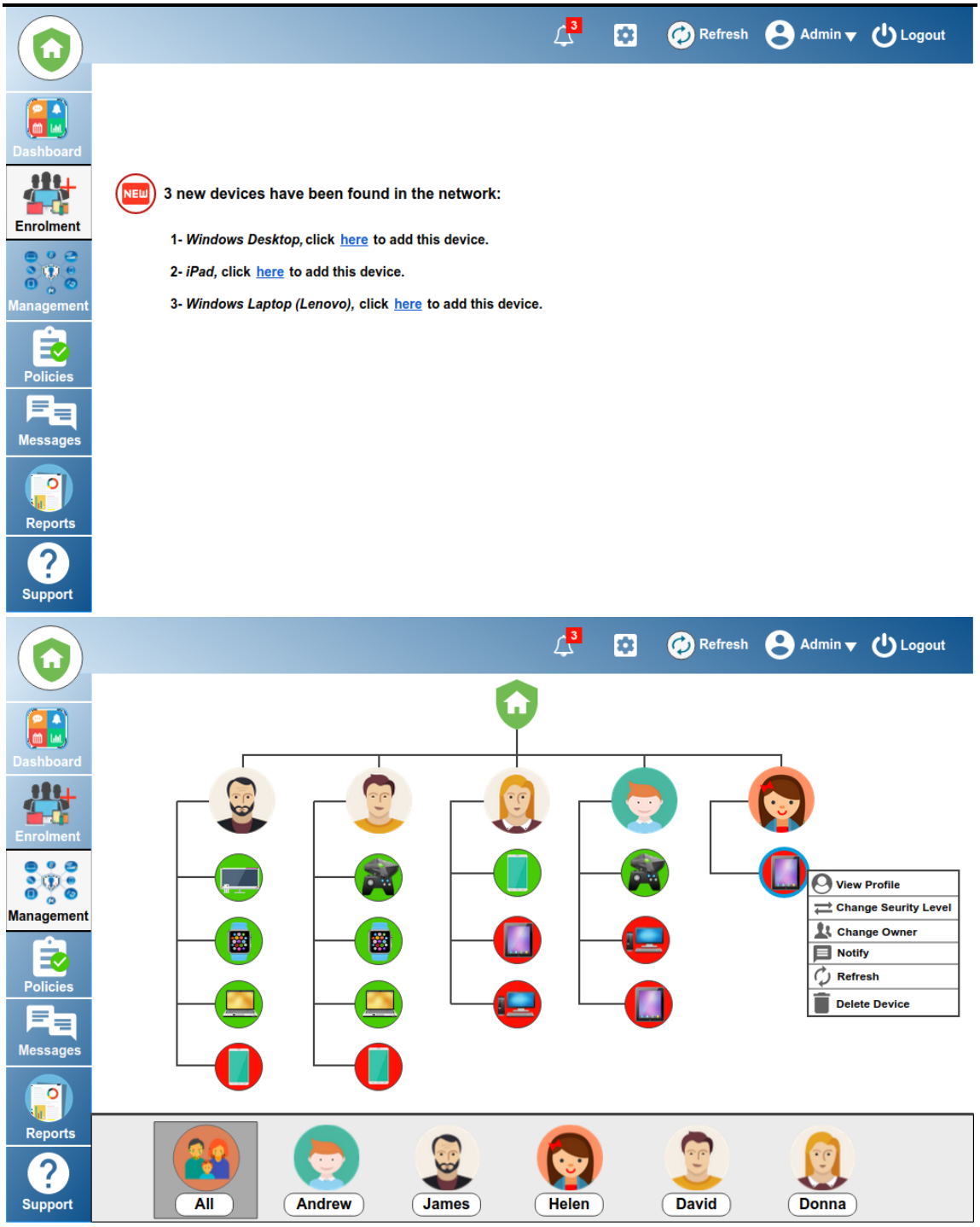

Refresh
Admin
Logout
Dashboard
Enrolment
Management
Policies
Messages
Reports
Support
Security Settings Alert
Cyber Hero of The Week
Activity Feed
Edit Widget
Data: Security Policies for All Devices
Select the policy to be shown
Password Policy
Device Security Policy
Software Policy
Internet Browser Policy
Backup Policy
Parental controls Policy
Type:
Non-Complaint Devices
Complaint Devices
Password Policy
Device Security Policy
Software Policy
Internet Browser Policy
Cancel
Save
View All
iPad
Send a message
Low
Security Level
Helen
Change Owner
Profile Summery
Enrolled
Compliant
IT Experience
Novice
Security Level
Low
Assigned Policies
5
No. reported issues
1
Last reported
6 hours ago
Hardware Inventory
Model: A1823 (5th generation)
Operating system IOS
Version: 11.0.1
IMEI:
Manufacturer: Apple
View All
Security Policies
Device Security
Internet Browser
Software
Backup
Parental control
Legitimate OS (installed)
Security Lock (enabled)
Fingerprint (enabled)
OS auto update (enabled)
Notification (enabled)
OS version is up-to-date
Time before auto-lock is 5 minutes
The configured security lock is PIN
Auto wipe after failed attempts (enabled)
Antivirus (enabled and updated)
SIM card PIN (enabled)
Locating the device (enabled)
Recent Activity
Non-complaint with parental control policy 1 day
Complaint with all the policies 2 days
Complaint with all the policies 5 days
Scan was successful 5 days
Enrolment was successfully 5 days
View all

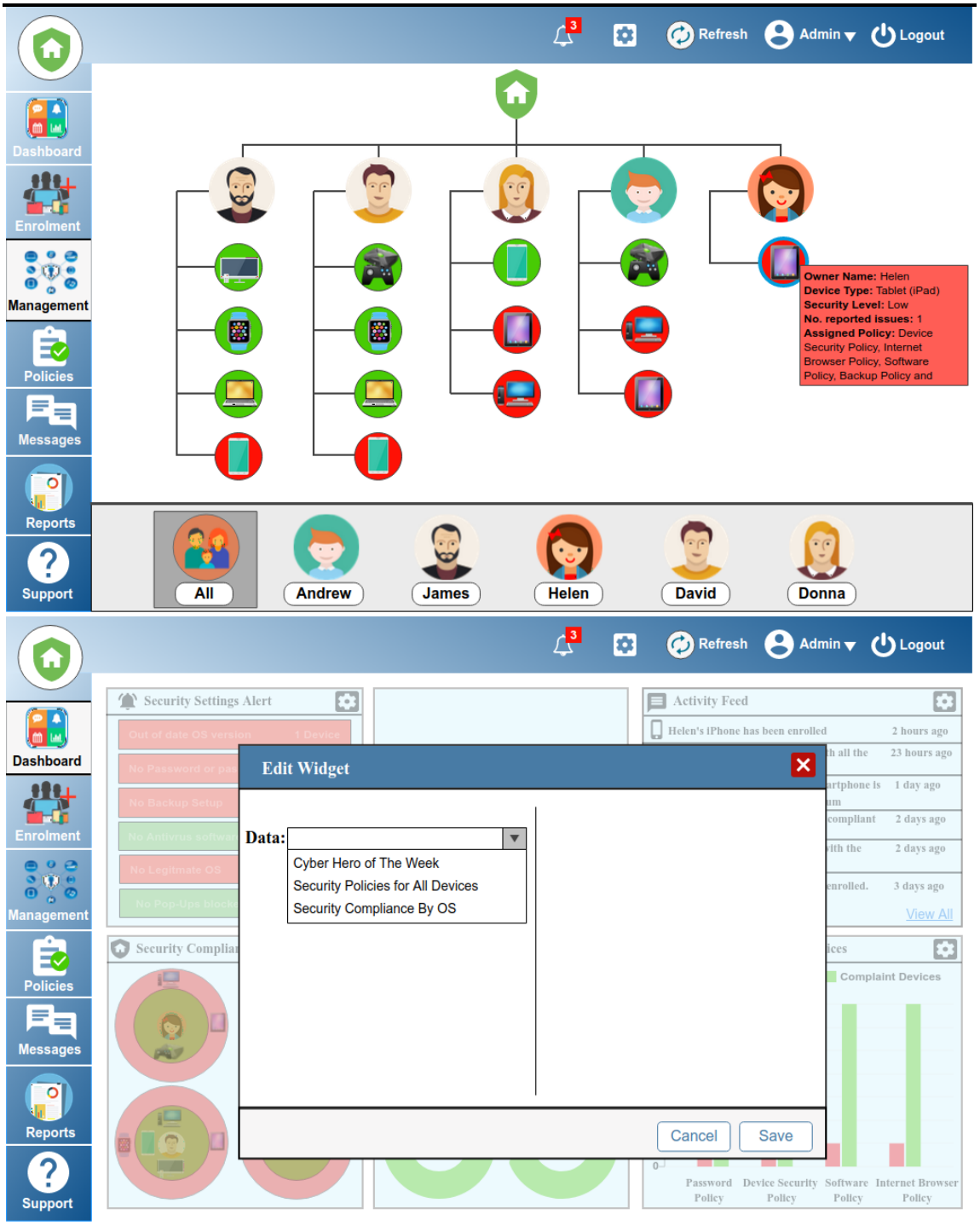

Refresh
Admin
Logout
Dashboard
Enrolment
Management
Policies
Messages
Reports
Support
Security Settings Alert
Cyber Hero of The Week
Activity Feed
Edit Widget
Data: Security Policies for All Devices
Select the policy to be shown
Password Policy
Device Security Policy
Software Policy
Internet Browser Policy
Backup Policy
Parental controls Policy
Type:
Non-Complaint Devices
Complaint Devices
Password Policy
Device Security Policy
Software Policy
Internet Browser Policy
Cancel
Save
View All
Refresh
James
Desktop
Devices
Notifications
Messages
Reports
Support
Profile Summary
Enrolled
Compliant
IT Experience
Novice
Security Level
Low
Assigned Policies
5
No. reported issues
0
Recent Activity
Device is complaint with all the policies 1 day
Device is complaint with all the policies 2 days
Device is not complaint with one policy 5 days
Device has been scanned successfully 5 days
Device has been enrolled successfully 5 days
View all
Do You Know ?
85% of cyber attacks are attributed to stolen credentials, keyloggers, social engineering, and phishing attacks – which all target passwords.
There have been at least 360,000 new malicious files such as viruses and malware detected every day in 2017 — an 11.5% increase from the previous year.
Unpdated operating systems and applications can be a major IT security risk. If you do not update your software it will leave your device and your network vulnerable to attackers.
Installing apps from unverified locations and sources can lead to issues with your device, and can potentially cause security problems.
For more information click here
Policy Compliance
Password Policy
Password (enabled)
Minimum Password Length (6 characters)
Enforce Password History (1 password)
Maximum Password Age (120 days)
Password Complexity (enabled)
Time before auto-lock (7 minutes)
Device Security Policy
Software Policy
Internet Browser policy
Backup Policy
Quiz of the week
What does the "https://" at the beginning of a URL denote, as opposed to "http://" (without the "s")?
The site has special high definition
Information entered into the site is encrypted
The site is the newest version available
The site is not accessible to certain computers
Submit
Top Users
1. Helen 2451
2. James 1569
3. Andrew 951
4. Donna 34

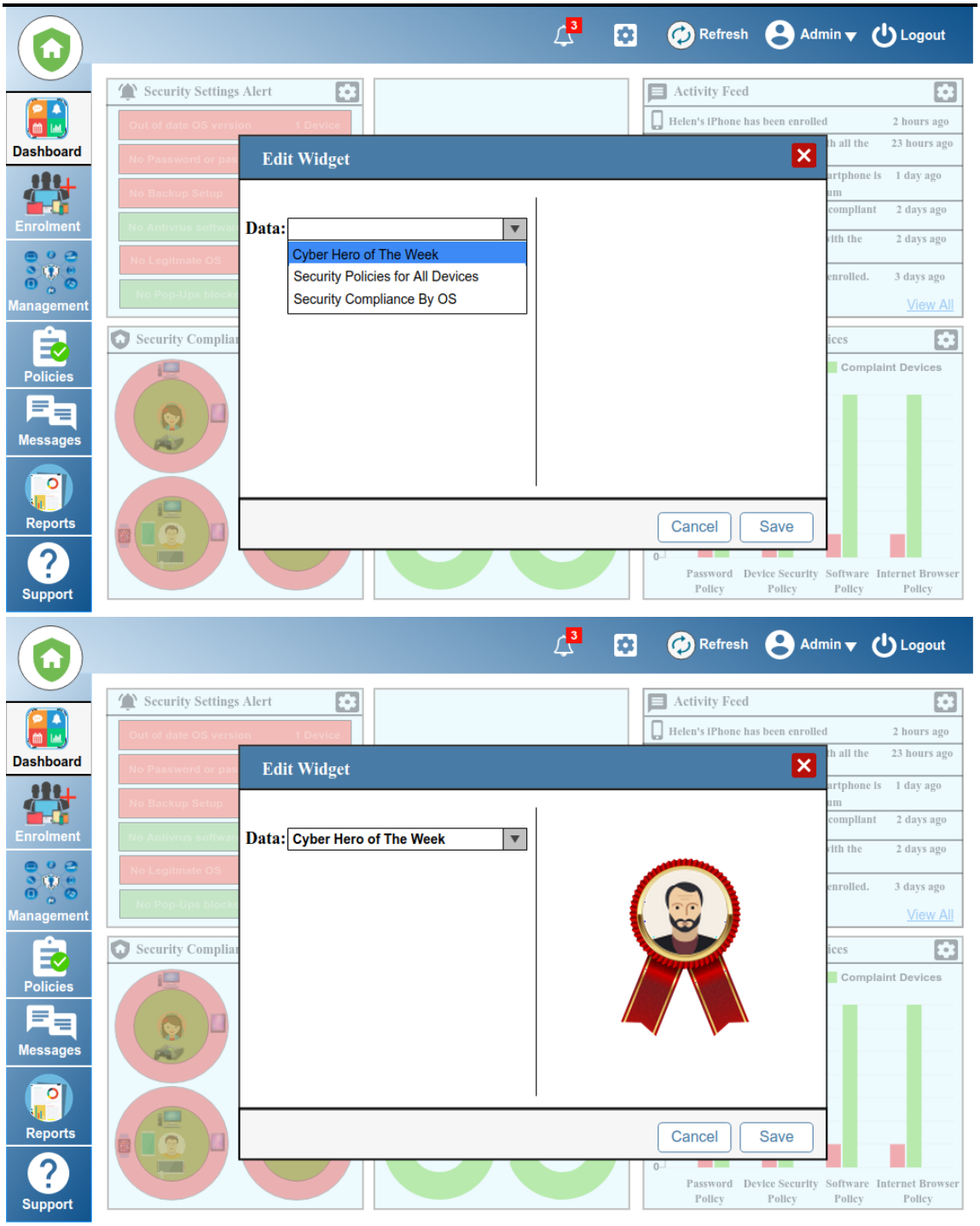

Refresh
Andrew
Laptop
Devices
Notifications
Messages
Reports
Support
Profile Summary
Enrolled
Compliant
IT Experience
Intermediate
Security Level
Medium
Assigned Policies
5
No. reported issues
1
Recent Activity
Device is not complaint with one policy 1 day
Device is complaint with all the policies 2 days
Device is not complaint with three policies 5 days
Device has been scanned successfully 5 days
Device has been enrolled successfully 5 days
View all
Do You Know ?
There have been at least 360,000 new malicious files such as viruses and malware detected every day in 2017 — an 11.5% increase from the previous year.
If your device doesn't have Anti-virus protection , you will be more vulnerable to viruses, malware, hackers and other different online threats.
Many viruses can be transferred to your device by using removable device such as USB sticks without being scanned by Anti-virus software.
For more information click here
Policy Compliance
Password Policy
Device Security Policy
Software Policy
Internet Browser policy
Backup Policy
Quiz of the week
Antivirus software protects your computer against which types of threats?
A program that could remotely control your computer
A program that could wipe out your data
A program that could steal your confidential information
All of the answers are correct
Submit
Top Users
1. Helen 2451
2. James 1569
3. Andrew 951
4. Donna 34

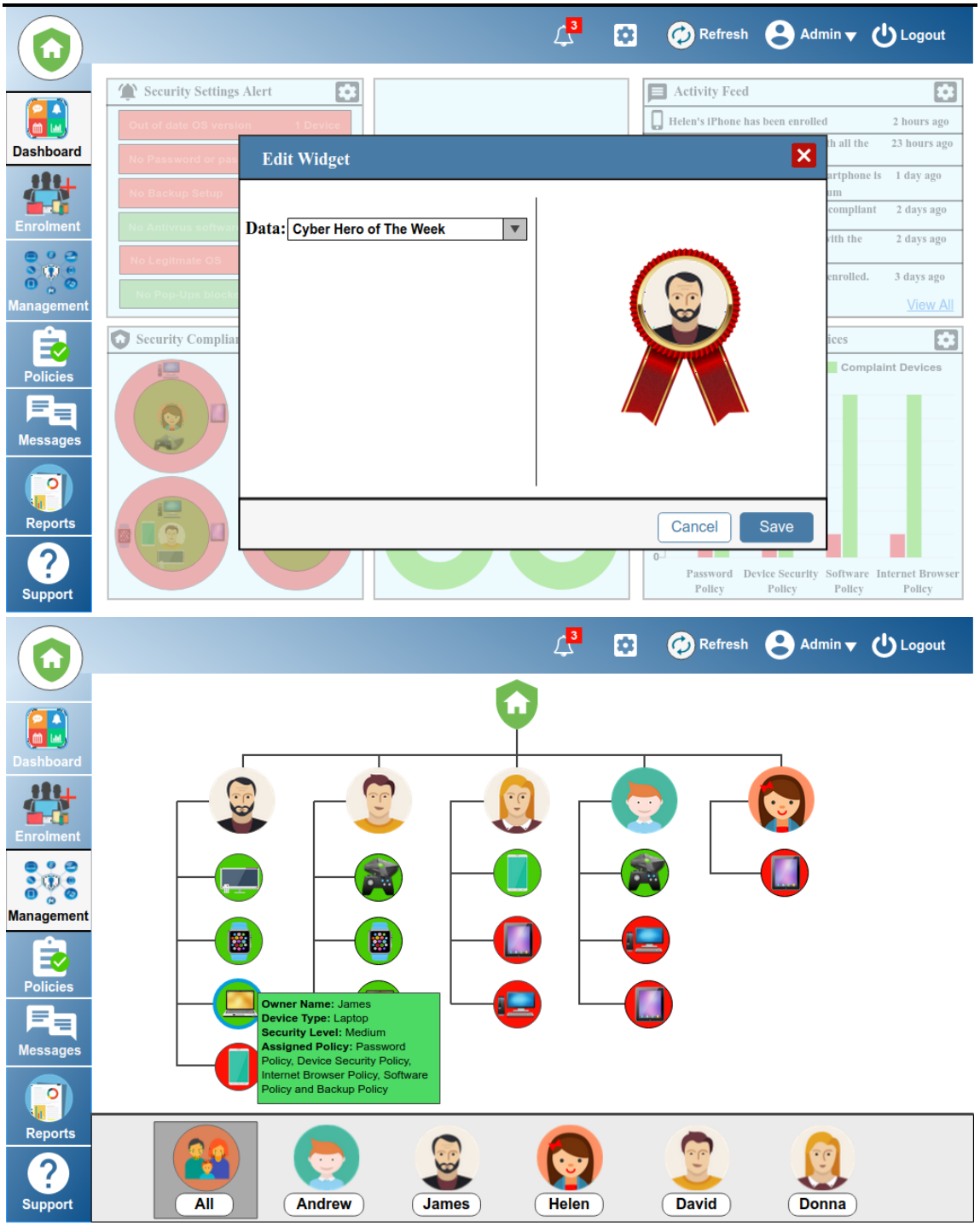

Refresh
Admin
Logout
Desktop PCs and Laptops Policy
Dashboard
Enrolment
Management
Policies
Messages
Reports
Support
Select the Security Level:
High
Medium
Low
Password Settings
Require Password Enabled
Minimum Password Length 12 Characters
Password Complexity Enabled
Maximum Password Age 60 days
Enforce Password History 3 Passwords
Account Lockout Threshold 5 Attempts
Account Lockout Duration 10 Minutes
Time before auto-lock 3 Minutes
Device Security Policy
Internet Browser Policy
Software Security Policy
Backup Policy
Parental Controls Policy

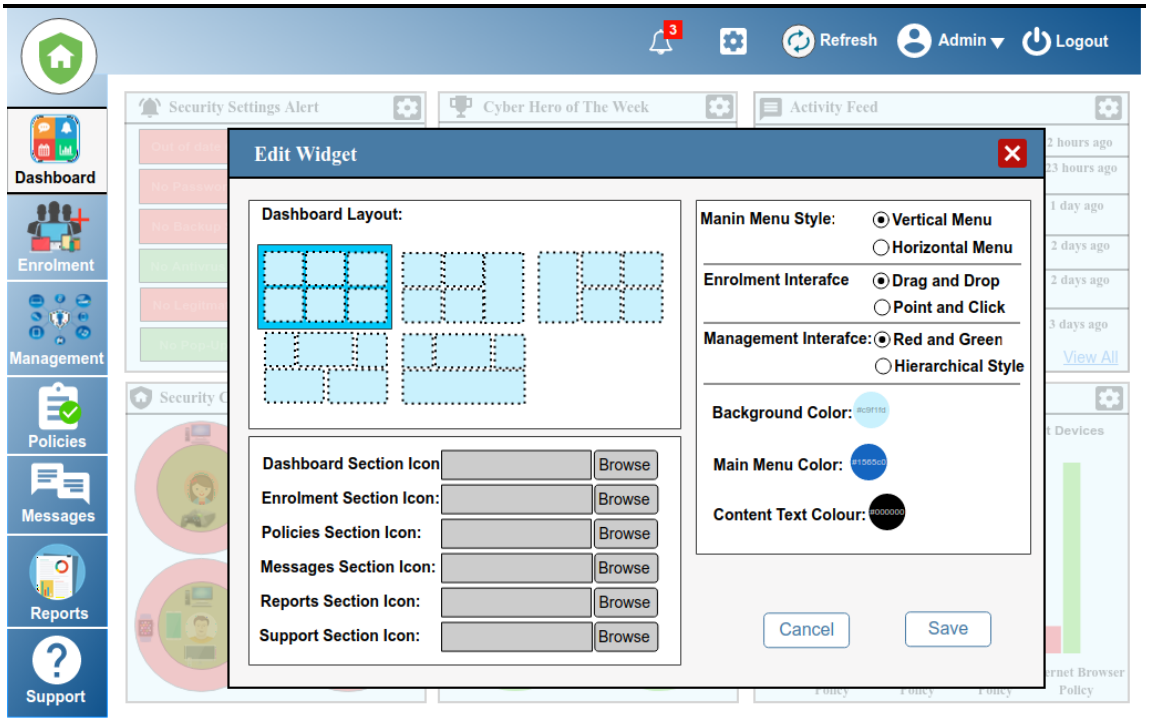

Refresh
Admin
Logout
Dashboard
Enrolment
Management
Policies
Messages
Reports
Support
Security Settings Alert
Activity Feed
Edit Widget
Data:
Cancel
Save
View All
Complaint Devices
Password Policy
Device Security Policy
Software Policy
Internet Browser Policy
iPad
Send a message
Low
Security Level
Helen
Change Owner
Profile Summery
Enrolled
Compliant
IT Experience
Novice
Security Level
Low
Assigned Policies
5
No. reported issues
1
Last reported
6 hours ago
Hardware Inventory
Model: A1823 (5th generation)
Operating system IOS
Version: 11.0.1
IMEI:
Manufacturer: Apple
View All
Security Policies
Device Security
Internet Browser
Software
Backup
Parental control
Parental control (enabled)
Time limit (enabled)
Apps limit (enabled)
Content and privacy restriction (disabled)
Recent Activity
Non-complaint with parental control policy 1 day
Complaint with all the policies 2 days
Complaint with all the policies 5 days
Scan was successful 5 days
Enrolment was successfully 5 days
View all

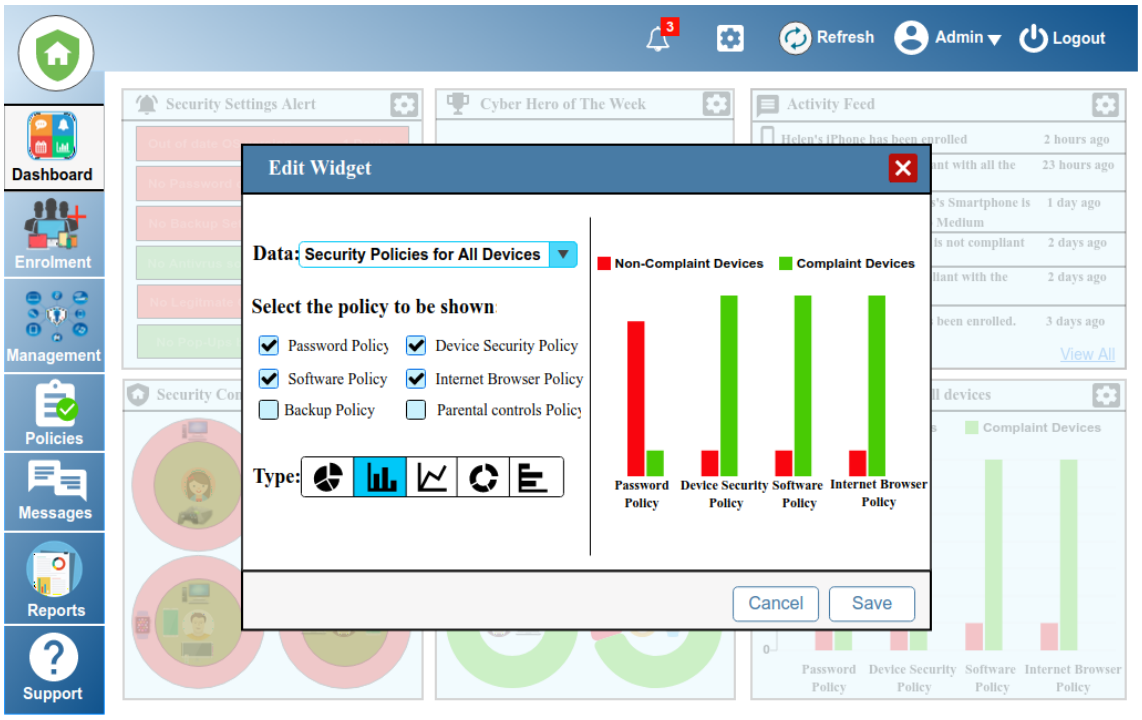

3
Refresh
Admin
Logout
Dashboard
Enrolment
Management
Policies
Messages
Reports
Support
NEW
3 new devices have been found in the network:
1- Windows Desktop, click here to add this device.
2- iPad, click here to add this device.
3- Windows Laptop (Lenovo), click here to add this device.
3
Refresh
Admin
Logout
Dashboard
Enrolment
Management
Policies
Messages
Reports
Support
View Profile
Change Seurity Level
Change Owner
Notify
Refresh
Delete Device
All
Andrew
James
Helen
David
Donna

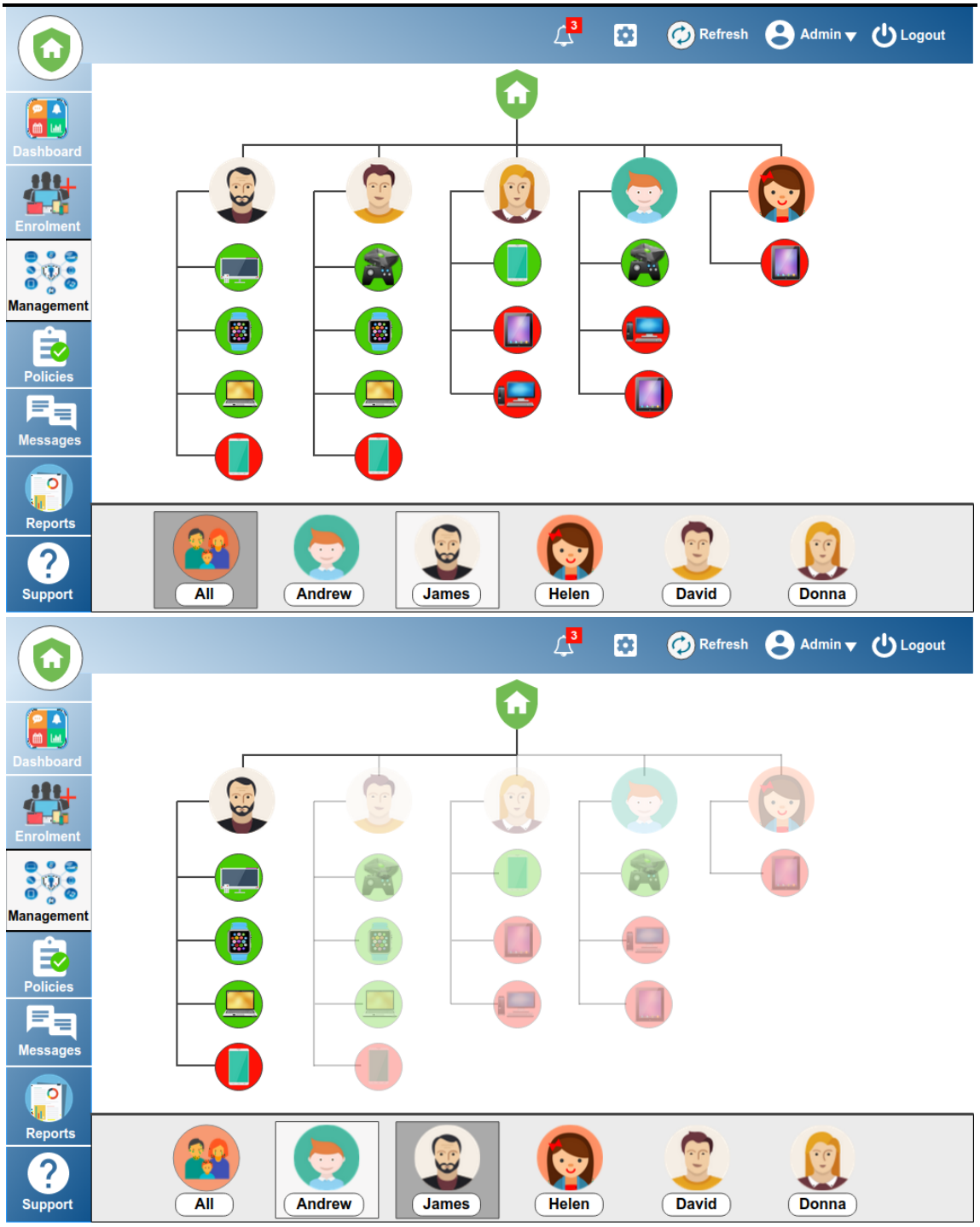

Refresh
Admin
Logout
Dashboard
Enrolment
Management
Policies
Messages
Reports
Support
Owner Name: Helen
Device Type: Tablet (iPad)
Security Level: Low
No. reported issues: 1
Assigned Policy: Device Security Policy, Internet Browser Policy, Software Policy, Backup Policy and
All
Andrew
James
Helen
David
Donna
Security Settings Alert
Activity Feed
Edit Widget
Data:
Cyber Hero of The Week
Security Policies for All Devices
Security Compliance By OS
Cancel
Save
Complaint Devices
Password Policy
Device Security Policy
Software Policy
Internet Browser Policy


Refresh
Admin
Logout
Dashboard
Enrolment
Management
Policies
Messages
Reports
Support
Security Settings Alert
Activity Feed
Edit Widget
Data:
Cyber Hero of The Week
Security Policies for All Devices
Security Compliance By OS
Cancel
Save
Complaint Devices
Password Policy
Device Security Policy
Software Policy
Internet Browser Policy
View All


Refresh
Admin
Logout
Dashboard
Enrolment
Management
Policies
Messages
Reports
Support
Security Settings Alert
Activity Feed
Edit Widget
Data:
Cyber Hero of The Week
Cancel
Save
Complaint Devices
Password Policy
Device Security Policy
Software Policy
Internet Browser Policy
Owner Name: James
Device Type: Laptop
Security Level: Medium
Assigned Policy: Password Policy, Device Security Policy, Internet Browser Policy, Software Policy and Backup Policy
All
Andrew
James
Helen
David
Donna


Refresh
Admin
Logout
Dashboard
Enrolment
Management
Policies
Messages
Reports
Support
Security Settings Alert
Cyber Hero of The Week
Activity Feed
Edit Widget
Dashboard Layout:
Manin Menu Style:
Vertical Menu
Horizontal Menu
Enrolment Interafce
Drag and Drop
Point and Click
Management Interafce:
Red and Green
Hierarchical Style
Background Color:
Main Menu Color:
Content Text Colour:
Dashboard Section Icon
Enrolment Section Icon:
Policies Section Icon:
Messages Section Icon:
Reports Section Icon:
Support Section Icon:
Browse
Cancel
Save


Refresh
Admin
Logout
Dashboard
Enrolment
Management
Policies
Messages
Reports
Support
Security Settings Alert
Cyber Hero of The Week
Activity Feed
Edit Widget
Data:
Security Policies for All Devices
Select the policy to be shown
Password Policy
Device Security Policy
Software Policy
Internet Browser Policy
Backup Policy
Parental controls Policy
Type:
Non-Complaint Devices
Complaint Devices
Password Policy
Device Security Policy
Software Policy
Internet Browser Policy
Cancel
Save


Refresh
Admin
Logout
Dashboard
Enrolment
Management
Policies
Messages
Reports
Support
All
Andrew
James
Helen
David
Donna
Refresh
Admin
Logout
Dashboard
Enrolment
Management
Policies
Messages
Reports
Support
All
Andrew
James
Helen
David
Donna